補正あり

(19)日本国特許庁（ＪＰ）　(12)**公表特許公報**（Ａ）　(11)特許出願公表番号

特表平10－501396

(43)公表日　平成10年(1998)２月３日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		
Ｈ０４Ｍ	3/00		9370－5G	Ｈ０４Ｍ	3/00	Ａ
	3/42		9567－5G		3/42	Ａ

審査請求　未請求　　予備審査請求　有　　(全 82 頁)

(21)出願番号　特願平8－502274
(86)(22)出願日　平成７年(1995)６月５日
(85)翻訳文提出日　平成８年(1996)12月６日
(86)国際出願番号　ＰＣＴ／ＵＳ９５／０７０７７
(87)国際公開番号　ＷＯ９５／３５６３３
(87)国際公開日　平成７年(1995)12月28日
(31)優先権主張番号　０８／２５４，５９０
(32)優先日　1994年６月６日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ベルサウス　コーポレイション
アメリカ合衆国，ジョージア　30367，アトランタ，ノースイースト，ピーチトゥリー　ストリート　1155番地
(72)発明者　ウェイサー，フランク，ジェイ．，ジュニア
アメリカ合衆国，ジョージア　30328，アトランタ，ハンターズ　トレース　サークル　6780番地
(74)代理人　弁理士　遠山　勉　（外３名）

最終頁に続く

(54)【発明の名称】　高度インテリジェントネットワークにおける呼量の取り次ぎ

(57)【要約】
市内交換会社が動作する高度インテリジェントネットワークと市内交換会社でないサービス・プロバイダーの間のインターフェースを通るデータパケットの呼量の取り次ぎの方法が開示される。このインターフェースは、サービス・プロバイダーと高度インテリジェントネットワークの間に、特に、サービス中継点（ＳＴＰ）等の市内交換会社の装置に接続されたＳＳ７プロトコルのデータリンクを通して高度インテリジェントネットワークへのアクセスを有するサービス制御点（ＳＣＰ）等のサービス・プロバイダーのネットワーク装置の間に規定される。ＳＴＰにおけるゲートウェイ・スクリーニングを用いて、市内交換会社でないネットワーク要素から発信されるデータパケットに関してある取り次ぎ手順が行われる。無効な値のデータパケットは拒絶されるが、妥当な値のデータパケットは通されて取り次ぎアクセスＳＣＰへのさらなる取り次ぎ手順に進む。データパケットの何らかのさらなる経路選択（データパケットの拒絶以外）の前に、取り次ぎアクセスＳＣＰは、データパケットのトランザクション番号等のデータパケットの発信源に関

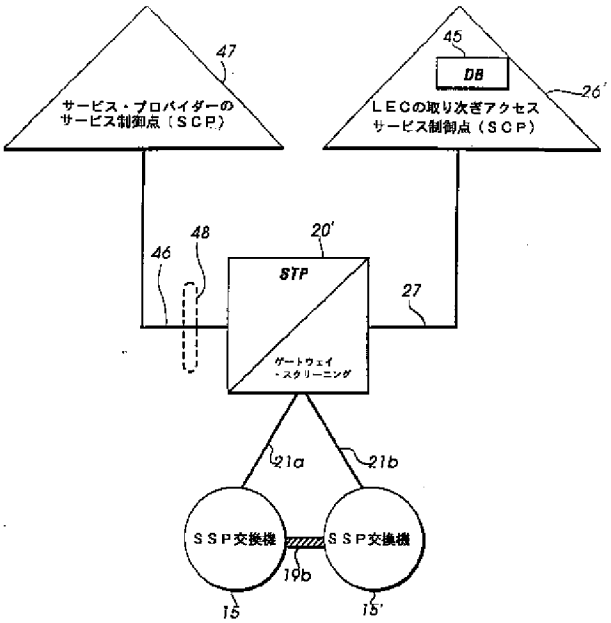

FIG 2

【特許請求の範囲】

１．サービス・プロバイダーのサービス制御点と、少なくとも１つの信号中継点と前記信号中継点に接続されている少なくとも１つの取り次ぎアクセスサービス制御点を含む複数のインテリジェント交換ネットワーク要素、の間での複数のデジタルデータ通信チャネルを含むインテリジェントな交換電話ネットワークの間で承認されないデータパケットメッセージの送信を防止する方法において、

前記信号中継点内でメッセージを受け取る手順、

前記メッセージを前記信号中継点から前記取り次ぎアクセスサービス制御点へと送信する手順、および

前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ手順

を含む方法。

２．前記取り次ぎアクセスサービス制御点が顧客の記録を含む少なくとも１つのデータベースを含み、前記メッセージが第１のトランザクション番号を含み、前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順が、

前記データベース内に前記メッセージのトランザクション識別子を記憶すること、

前記メッセージの第２のトランザクション番号を生成すること、

前記第２のトランザクション番号を前記データベース内の前記第１のトランザクション識別子と関連づけること、

前記第１のトランザクション番号を前記メッセージから取り去ること、および

前記第２のトランザクション番号を前記メッセージに付け加えること

を含む、請求の範囲第１項記載の方法。

３．前記トランザクション識別子を記憶する前に、前記メッセージをメッセージ情報として読み取る手順、

前記メッセージ情報を、前記データベース内の少なくとも１つの顧客の記録に対応するか比較する手順、および

前記メッセージ情報が前記顧客の記録と対応しない場合には、前記メッセージを拒絶する手順

をさらに含む、請求の範囲第２項記載の方法。

４．前記トランザクション識別子が、前記第１のトランザクション番号、前記メッセージの発信点コード、および前記メッセージのサブシステム番号を含み、前記トランザクション識別子を記憶する前記手順が、前記第１のトランザクション番号、前記発信点コード、および前記サブシステム番号を記憶することを含む、請求の範囲第２項記載の方法。

５．前記メッセージが、前記第１のトランザクション番号、前記発信点コード、および前記サブシステム番号を含み、前記第１のトランザクション番号を取り去る前記手順が、前記第１のトランザクション番号、前記発信点コード、および前記サブシステム番号を前記メッセージから取り去ることを含む、請求の範囲第４項記載の方法。

６．前記第２のトランザクション番号を前記データベース内の活動状態の第２のトランザクション番号のリスト内に記憶する手順をさらに含む、請求の範囲第３項記載の方法。

７．前記第２のトランザクション番号が割り当てられていない疑似乱数であり、前記第２のトランザクション番号を生成する前記手順が、前記割り当てられていない疑似乱数を前記第２のトランザクション番号として生成することを含む、請求の範囲第３項記載の方法。

８．前記取り次ぎアクセスサービス制御点が顧客の記録を含む少なくとも１つのデータベースを含み、前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順が、

前記メッセージが応答メッセージであるかどうかを決定すること、

前記メッセージが応答メッセージである場合には、前記応答メッセージのトランザクション番号を前記データベース内の活動状態のトランザクション番号のリストに対応するか比較すること、および

前記トランザクション番号が活動状態のトランザクション番号の前記リスト内の入力と対応しない場合には、前記メッセージを拒絶すること

を含む、請求の範囲第１項記載の方法。

９．前記トランザクション番号が活動状態のトランザクション番号の前記リスト内の入力と対応する場合には、前記入力から受信宛先情報を取得する手順、およ

び

前記受信宛先情報をベースにして前記メッセージの経路を選択する手順

をさらに含む、請求の範囲第８項記載の方法。

１０．前記メッセージが、照会メッセージに応答して前記サービス・プロバイダーのサービス制御点から受け取られる応答メッセージであり、前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順が、

前記応答メッセージが発信点コードを含むかどうかを決定すること、

前記応答メッセージが前記発信点コードを含む場合には、前記発信点コードを前記照会メッセージと関連する受信宛先点コードに対応するか比較すること、および

前記発信点コードが前記受信宛先点コードに対応しない場合には、前記メッセージを拒絶すること

を含む、請求の範囲第１項記載の方法。

１１．前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順の後の、前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次がれなかったかどうかを決定する手順、および

前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次がれなかった場合には、前記メッセージを拒絶して前記メッセージにデフォルト応答を供給する手順

をさらに含む、請求の範囲第１項記載の方法。

１２．前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次ぐ前記手順の後の、前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次ぎにパスしたかどうかを決定する手順、および

前記メッセージが前記取り次ぎアクセスサービス制御点内で取り次ぎにパスした場合には、前記サービス・プロバイダーのサービス制御点がアウトオブサービスであるかどうかを決定する手順、および

前記サービス・プロバイダーのサービス制御点がアウトオブサービスである場合には、前記メッセージを拒絶して前記メッセージにデフォルト応答を供給する手順

をさらに含む、請求の範囲第１項記載の方法。

１３．前記メッセージが特定のサービス・プロバイダーのサービスの要求を含み、前記サービス・プロバイダーのサービス制御点がアウトオブサービスであるかどうかを決定する前記手順が前記特定のサービス・プロバイダーのサービスがアウトオブサービスであるかどうかを決定すること、および

前記特定のサービス・プロバイダーのサービスがアウトオブサービスである場合には、前記メッセージを拒絶して前記メッセージにデフォルト応答を供給すること

を含む、請求の範囲第１２項記載の方法。

１４．前記信号中継点内でメッセージを受け取る手順の後の、前記メッセージが前記サービス・プロバイダーの信号制御点から発信されているかどうかを決定する手順、および

前記メッセージが前記サービス・プロバイダーの信号制御点から発信されている場合には、最初に前記信号中継点内で前記メッセージを取り次ぐ手順

をさらに含む、請求の範囲第１項記載の方法。

１５．前記メッセージが発信点コードを含み、前記信号中継点が前記信号中継点へのメッセージのそれぞれの承認されたプロバイダーのポート識別子を有し、最初に前記信号中継点内で前記メッセージを取り次ぐ前記手順が

前記発信点コードが少なくとも１つのポート識別子に対応するか比較すること、および

前記発信点コードが前記ポート識別子のいずれにも対応しない場合には、前記メッセージを拒絶すること

を含む、請求の範囲第１４項記載の方法。

１６．前記メッセージが受信宛先コードを含み、前記信号中継点が前記信号中継点へのメッセージのそれぞれの承認されたプロバイダーのメッセージの承認された受信宛先を指定する少なくとも１つの承認されたアドレスを有し、最初に前記信号中継点内で前記メッセージを取り次ぐ前記手順が

前記受信宛先コードが少なくとも１つの承認されたアドレスに対応するか比較すること、および

前記受信宛先コードが前記承認されたアドレスのいずれにも対応しない場合には、前記メッセージを拒絶すること
を含む、請求の範囲第１４項記載の方法。
１７．前記承認されたアドレスの１つが前記取り次ぎアクセスサービス制御点のアドレスを含み、前記比較する手順が前記受信宛先コードが前記取り次ぎアクセスサービス制御点の前記アドレスに対応するか比較することを含み、前記拒絶する手順が前記受信宛先コードが前記取り次ぎアクセスサービス制御点の前記アドレスに対応しない場合には前記メッセージを拒絶することを含む、請求の範囲第１６項記載の方法。
１８．前記メッセージがサービスインジケータを含み、前記信号中継点が前記信号中継点へのメッセージのそれぞれの承認されたプロバイダーの承認されたサービスを指定する少なくとも１つのサービスインジケータを有し、最初に前記信号中継点内で前記メッセージを取り次ぐ前記手順が
前記サービスインジケータが少なくとも１つの承認されたサービスインジケータに対応するか比較すること、および
前記サービスインジケータが前記承認されたサービスインジケータのいずれにも対応しない場合には、前記メッセージを拒絶すること
を含む、請求の範囲第１４項記載の方法。
１９．複数のネットワーク要素の間の複数のデジタルデータ通信チャネルを含むインテリジェント交換電話ネットワークにおけるパケットメッセージの呼量を取り次ぐ方法において、
前記複数のネットワーク要素のうちで新しいＴＣＡＰメッセージを生成する第１のものにそれぞれの前記新しいＴＣＡＰメッセージについて第１のトランザクション番号を生成させる手順、
前記複数のネットワーク要素のうちの第２のものに前記ＴＣＡＰメッセージを送信する前記第１のネットワーク要素の前に、前記第１のネットワーク要素に前記第１のトランザクション番号を前記ＴＣＡＰメッセージ内に含ませる手順、
前記第２のネットワーク要素に前記ＴＣＡＰメッセージの単一のトランザクション識別子を作り出させる手順、

前記第２のネットワーク要素に前記ＴＣＡＰメッセージの第２のトランザクション番号を生成させる手順、

前記第２のネットワーク要素に前記ＴＣＡＰメッセージから前記第１のトランザクション番号を削除させる手順、

別の受信宛先に前記ＴＣＡＰメッセージを送信する前記ネットワーク要素の前に、前記第２のネットワーク要素に前記ＴＣＡＰメッセージ内の前記第２のトランザクション番号を含ませる手順、および

前記ネットワーク要素に、前記ＴＣＡＰメッセージと関連する特定のトランザクションに影響を与えるが内部に前記第２のトランザクション番号は含んでいない他のＴＣＡＰメッセージをその後拒絶させる手順

を含む方法。

２０．前記第１のネットワーク要素に、トランザクション識別子のテーブル内に前記第１のトランザクション番号を記憶させる手順

をさらに含む、請求の範囲第１９項記載の方法。

２１．前記第２のネットワーク要素に、トランザクション識別子のテーブル内に前記単一のトランザクション識別子を記憶させる手順、および

前記第２のネットワーク要素に、前記単一のトランザクション識別子と関連して前記トランザクション識別子のテーブル内に前記第２のトランザクション番号を記憶させる手順

をさらに含む、請求の範囲第１９項記載の方法。

２２．前記第１のネットワーク要素に前記第１のトランザクション番号を含ませる前記手順が、前記第１のネットワーク要素に前記ＴＣＡＰメッセージ内に前記第１のトランザクション番号およびメッセージ識別子を含ませることを含む、請求の範囲第１９項記載の方法。

２３．前記ＴＣＡＰメッセージが発信点コードおよびサブシステム番号を含み、前記第２のネットワーク要素に前記単一のトランザクション識別子を作り出させる前記手順が、前記第１のトランザクション番号を前記発信点コードおよび前記サブシステム番号と連結することによって前記第２のネットワーク要素に前記単一のトランザクション識別子を作り出させることを含む、請求の範囲第２３項記

載の方法。

２４．前記第２のネットワーク要素に前記第１のトランザクション番号を削除させる前記手順が、前記第２のネットワーク要素に前記ＴＣＡＰメッセージから前記第１のトランザクション番号、前記発信点コード、および前記サブシステム番号を削除させることを含む、請求の範囲第２３項記載の方法。

２５．サービス・プロバイダーのサービス制御点と、複数のネットワーク要素の間の複数のデジタルデータ通信チャネルを含むインテリジェント交換電話ネットワークの間の、パケットメッセージの呼量を取り次ぐ方法において、

第１のトランザクション番号を有するメッセージを受け取るネットワーク要素に前記メッセージと関連して単一のトランザクション識別子を作り出させる手順、

前記ネットワーク要素に前記メッセージの第２のトランザクション番号を生成させる手順、

前記ネットワーク要素に前記単一のトランザクション識別子に関連して前記第２のトランザクション番号を記憶させる手順、

前記ネットワーク要素に前記メッセージから前記第１のトランザクション番号を削除させる手順、

前記ネットワーク要素に、前記メッセージに前記第２のトランザクション番号を付け加えさせる手順、および

前記サービス・プロバイダーのサービス制御点および前記ネットワーク要素に、その後、前記メッセージと関連する特定のトランザクションに影響を与える他のメッセージ内の前記第２のトランザクション番号を含ませ、前記第２のトランザクション番号を含んでいない前記他のメッセージを拒絶させる手順

を含む方法。

２６．前記メッセージが発信点コードを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージのそれぞれの承認されたプロバイダーのポート識別子を有し、

前記ネットワーク要素に前記発信点コードが１つのポート識別子に対応するか比較させる手順、

前記発信点コードが前記ポート識別子のいずれにも対応しない場合には、前記

ネットワーク要素に前記メッセージを拒絶させる手順

をさらに含む、請求の範囲第２５項記載の方法。

２７．前記メッセージが受信宛先コードを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージのそれぞれの承認されたプロバイダーのメッセージの承認された受信宛先を指定する少なくとも１つの承認されたアドレスを有し、

前記ネットワーク要素に前記受信宛先コードが少なくとも１つの承認されたアドレスに対応するか比較させる手順、

前記受信宛先コードが前記承認されたアドレスのいずれにも対応しない場合には、前記ネットワーク要素に前記メッセージを拒絶させる手順

をさらに含む、請求の範囲第２５項記載の方法。

２８．前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージのそれぞれの承認されたプロバイダーの承認されたサービスを指定する少なくとも１つのサービスインジケータを有し、

前記ネットワーク要素に前記サービスインジケータが少なくとも１つの承認されたサービスインジケータに対応するか比較させる手順、

前記サービスインジケータが前記承認されたサービスインジケータに対応しない場合には、前記ネットワーク要素に前記メッセージを拒絶させる手順

を含む、請求の範囲第２５項記載の方法。

２９．サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点の法定の中継回線のグループのインデックスのテーブルを維持させる手順、

前記ある特定の中継回線のグループの経路選択の要求を含むメッセージを受け取る前記取り次ぎアクセスサービス制御点に応答して、前記取り次ぎアクセスサ

ービス制御点に前記特定の中継回線のグループの経路選択に対応する入力の前記テーブルをチェックさせる手順、および

前記特定の中継回線のグループの経路選択が前記テーブル内の入力に対応しない場合には、前記取り次ぎアクセスサービス制御点に前記メッセージを拒絶させる手順

を含む方法。

３０．サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点のネットワーク要素の承認された加入者電話番号のテーブルを維持させる手順、

ネットワーク要素へのアクセスの要求を含むメッセージを受け取る前記取り次ぎアクセスサービス制御点に応答して、前記取り次ぎアクセスサービス制御点に前記ネットワーク要素の加入者電話番号に対応する入力の前記テーブルをチェックさせる手順、および

前記加入者電話番号が前記テーブル内の入力に対応しない場合には、前記取り次ぎアクセスサービス制御点に前記メッセージを拒絶させる手順

を含む方法。

３１．サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点の許された資源占有数を維持させる手順、

前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点が占有している資源の現在のカウントを維持させる手順、

ネットワーク資源の使用の要求を含むメッセージを受け取る前記取り次ぎアクセスサービス制御点に応答して、前記現在のカウントが前記許された資源占有数

と等しいかそれよりも大きい場合には、前記取り次ぎアクセスサービス制御点に前記メッセージを拒絶させる手順
を含む方法。
３２．サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス

制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、
前記取り次ぎアクセスサービス制御点に、前記サービス・プロバイダーのサービス制御点が予め選択した期間内に戻さないメッセージの現在のカウントを維持させる手順、
前記現在のカウントが予め選択したカウントと等しいかそれよりも大きい場合には、前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点に供給されるメッセージの数を減らさせる手順
を含む方法。
３３．前記取り次ぎアクセスサービス制御点にメッセージの数を減らさせる前記手順が、前記取り次ぎアクセスサービス制御点に前記サービス・プロバイダーのサービス制御点に向けられた次のメッセージを拒絶させることを含む、請求の範囲第３２項記載の方法。
３４．前記ネットワークが前記サービス・プロバイダーのサービス制御点をサービスする少なくとも１つのサービス交換点を含み、前記取り次ぎアクセスサービス制御点にメッセージの数を減らさせる前記手順が、前記取り次ぎアクセスサービス制御点に自動発呼ギャッピングのメッセージを前記サービス交換点に送らせることを含む、請求の範囲第３２項記載の方法。
３５．前記アウトオブサービスのサービス・プロバイダーのサービス制御点をテストする手順、
前記アウトオブサービスのサービス・プロバイダーのサービス制御点が前記テストに適切に応答する場合、前記アウトオブサービスのサービス・プロバイダーのサービス制御点を使用可能状態のサービス・プロバイダーのサービス制御点として再分類する手順

をさらに含む、請求の範囲第１２項記載の方法。

３６．前記アウトオブサービスのサービス制御点をテストする前記手順が、前記アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを送ることを含む、請求の範囲第３５項記載の方法。

３７．前記アウトオブサービスのサービス制御点をテストする前記手順が、前記

アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを定期的なベースで送ることを含む、請求の範囲第３６項記載の方法。

３８．アウトオブサービスのサービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを送る手順、

前記アウトオブサービスのサービス・プロバイダーのサービス制御点が前記テストメッセージに適切に応答する場合、前記アウトオブサービスのサービス・プロバイダーのサービス制御点を使用可能状態のサービス・プロバイダーのサービス制御点として再分類する手順

を含む方法。

３９．前記アウトオブサービスのサービス制御点にテストメッセージを送る前記手順が、前記アウトオブサービスのサービス・プロバイダーのサービス制御点にテストメッセージを定期的なベースで送ることを含む、請求の範囲第３８項記載の方法。

４０．サービス・プロバイダーのサービス制御点と、取り次ぎアクセスサービス制御点を含むインテリジェント交換電話ネットワークの間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記取り次ぎアクセスサービス制御点に、データパケットメッセージ内の前記取り次がれた呼量に関する監査できる事象を認識させる手順、

前記監査できる事象の監査証跡を作り出す手順

を含む方法。

４１．前記監査できる事象がメッセージを含み、前記監査証跡が、日付、時間、トリガのタイプ、および前記メッセージのトリガする受信宛先番号および前記メッセージの写し、を含み、前記監査できる事象の監査証跡を作り出す前記手順が、前記日付、前記時間、前記トリガのタイプ、および前記メッセージの前記トリガする受信宛先および前記メッセージの前記写し、を含む前記監査証跡を作り出すことを含む、請求の範囲第４０項記載の方法。

４２．サービス・プロバイダーのサービス制御点と、インテリジェント交換電話ネットワーク内の複数のネットワーク要素の間の、データパケットメッセージの取り次がれた呼量を管理する方法において、

前記ネットワーク要素のうちの１つ内に、セキュリティ監査要求のパラメータを含むメッセージを受け取る手順、および

前記セキュリティ監査要求のパラメータを受け取ることに応答して、前記ネットワーク要素のうちの前記１つに前記メッセージのセキュリティ・パラメータを作り出させる手順

を含む方法。

４３．前記ネットワーク要素に、その後前記メッセージと関連する特定のトランザクションに影響を与える他のメッセージのある(with)前記セキュリティ・パラメータを含ませる手順

をさらに含む、請求の範囲第４２項記載の方法。

【発明の詳細な説明】

高度インテリジェントネットワークにおける呼量の取り次ぎ

関連出願の相互参照

この出願は、発明の名称「公衆電話ネットワーク用のオープンな高度インテリジェントネットワークのインターフェースの取り次ぎ」に係る１９９３年６月２８日提出の合衆国特許出願第０８３、９８４号の一部継続出願であり、且つ、発明の名称「共同命令実行環境によるオープンな高度インテリジェントネットワークのインターフェースの取り次ぎ」に係る１９９４年５月２０日提出の合衆国特許出願（出願人代理人整理番号１９２６０－０４１０）の一部継続出願である。本出願人はこの参照により、同時に係属し、且つ、共有された上記特許出願を併合する。

技術分野

本発明は、交換式電話による通信の分野に関し、特に、現代の電話交換システムに関連する高度インテリジェントネットワーク（ＡＩＮ:Advanced Intellgent Network）へのアクセスを電話サービス・プロバイダー以外の広範囲のエンティティに与えることによって許されるであろうメッセージ内容およびネットワークの影響の取り次ぎの方法である。

背景技術

米国において電話サービスが利用できるようになってからの１世紀余りの間に、公衆電話システムの複雑さ、大きさ、および性能は、絶えず発展し発達してきた。発呼を交換し完了する配線盤を操作する人間のオペレータによって発呼の経路が選択されてきた時代から、システムの容量は、呼量においてもサービスのオプションの量においても非常に増してきた。電話会社の電話局または電話局交換機は、それぞれが顧客の電話装置を終端とする多数の加入者回線が接続される装置である。従来の住居用の電話サービスについては、加入者回線には１個またはそれ以上の電話機が接続される。さらに電話局は、その電話局を他の電話局に接続する

多数の中継回線を有する。事務所に構内交換機（ＰＢＸ: private branch excha

nge）の交換機を供給する中継回線等の他の中継回線も、顧客に提供されている。

改善された電話サービスの初期の発展のひとつは、１９６０年代初期における加入者長距離市外ダイヤル方式の導入である。それ以前は、長距離市外通話はすべて、１人またはそれ以上の人間のオペレータが取り扱わねばならず、オペレータが呼線を設定しビリング装置を起動していた。加入者長距離市外ダイヤル方式を可能にした技術の重要な特徴のひとつは、ダイヤルされたディジットすなわち被呼番号を識別するデータを集め、記憶し、転送する交換機の性能である。これらは、発呼が多周波（ＭＦ：multifrequency）信号としてよく知られている信号体系を経由して設定されるときに、ネットワークを通して伝送された。ＭＦ信号は、情報信号（被呼番号を識別するもの）が、いったん発呼が完了すると音声信号を搬送する中継回線と同じ中継回線を介して、音声周波数帯域内の信号によって伝送された、という点において、帯域内周波信号方式の１種である。この技術によって、取り扱われる長距離の呼量がずっと多くなり、１９６０年代および１９７０年代の米国において電話サービスをかなり改良しより多くのサービスを求める要求を満たす助けとなった。帯域内周波信号方式技術の主な欠点は、発呼の設定の間、音声中継容量(voice trunk capacity)が占有される、ということであった。さらに、相手側の発呼番号が話し中である等何らかの理由によって発呼を完了することができない場合、発呼の設定がネットワークを通るその道筋を切り替えて話し中の報告が音声回線を介して発呼者に戻される間、長距離の中継容量が占有されてしまった。５分から１０分でも、１日に何千もの話し中の通話があると、中継容量をかなり使用することになる。

１９７０年代の後期および１９８０年代の初期において、米国電話電信会社（ＡＴ＆Ｔ：American Telephone & Telegraph Company）は初期の種類のオフィス間共通線信号方式（ＣＣＩＳ：common channel interoffice signaling）を開発した。ＣＣＩＳは、本質的に、電話の発呼についての情報が、発呼自体の信号の伝送に用いられる音声回線とは別個の高速データリンクを介して伝送される、交換電話ネットワークのネットワーク・アーキテクチャである。オフィス間共通線信号方式の開発の初期においては、音声リンクを設定する中継回線容量を割り

当てる前に発呼を完了できるかどうかを最初に決定することができる高速デジタルデータを提供するように、オフィス間データ信号リンクを設計することができると認識されていた。従って、オフィス間共通線信号方式では、アトランタにいる発呼者がシアトルの番号をダイヤルする場合には、被呼番号の識別を、アトランタにある発呼側の電話局からシアトルにある被呼側の電話局にオフィス間信号データリンクを介して伝送することができる。被呼側の電話局は、被呼番号にサービスを提供する電話局である。被呼番号が話し中の場合には、この情報を提供するデータがオフィス間信号リンクを介してアトランタにある発呼側の電話局に伝送で戻され、このアトランタにある電話局が、市内で話し中音を発呼者に提供する。従って、この処理の間に長距離中継回線容量が占有されることはなく、以前の方式であれば発呼を完了しようとして用いられたであろうアトランタとシアトルの間の音声回線は、他の使用への余地を残している。シアトルの被呼番号が話し中でない場合には、ネットワーク内の様々な装置がこの発呼に関する情報に応答し、その発呼の接続を設定するオフィス間中継回線が割り当てられ、発呼が完了する。

公衆電話ネットワークは、１９８０年代に、複合的で非常に用途が多いシステムに発展した。その大部分は、オフィス間共通線信号方式の１形式をサポートし、それによって制御されている。このネットワークの基礎は、ＡＴ＆Ｔが設計した。司法的な命令により１９８４年にＡＴ＆Ｔが市内交換会社(ＬＥＣ：local exchange carriers)を分割してからは、ベル地域経営会社(ＲＢＯＣ: Regional Bell Operating Companies)その他独立した市内電話サービス・プロバイダーがこのネットワークの開発を継続している。交換電話ネットワークの基本アーキテクチャは、かなりの部分において、米国、および西ヨーロッパや日本を含む先進工業化世界全体にわたって、同一である。本明細書で説明する現在のネットワークの詳細は、ＲＢＯＣその他米国内で操業している市内交換会社が用いているものである。このネットワーク・アーキテクチャは、米国における現代の電話交換システムのすべてが用いており、西ヨーロッパおよび日本における現代のシステムと略同一である。

現代のオフィス間信号は、信号方式７（ＳＳ７: signaling system ７）と呼

ば

れるプロトコルを用いてデジタルリンクを介して起こる。ＳＳ７については、以下により詳細に触れる。高度インテリジェントネットワーク（ＡＩＮ:Advanced Intellgent Network）は、以下の特性を有しているという点において、現在のオフィス間信号の拡張集合とみなしてもよい。第一に、これもＳＳ７プロトコルを用いている。基本的に、高度インテリジェントネットワークは、トリガとして知られているＡＩＮメッセージを生成し適切な応答を行う資源および相互接続を集めたものである。トリガとは、新しいＡＩＮメッセージ・シーケンスを生成するある特定の事象である。市内交換会社の顧客は、ある特定のトリガの事象に関してＡＩＮに提供されるトリガを有することに対して料金を支払わねばならない。例えば、ある番号への着信に関する特殊なサービスを受けるためには、その加入者電話番号の顧客は通常、成端試みトリガ(termination attempt trigger)を契約せねばならない。これによって、誰か加入者がその特定の加入者電話番号に通話を申し込もうとしたことをネットワークが検出するときにはいつでも、ＡＩＮメッセージが生成される。すると、サービス制御点がデータベースに情報を求め、トリガが受け取られたことを考えればその発呼の取り扱いについてどのような非標準の応答が適切であるかを決定する。米国において電話事業に精通した人々の多くが近い将来に起こると考えている次のような出来事の結果として、本発明が必要となる。すなわち、市内交換会社が動作する高度インテリジェントネットワークへのアクセスが第三者に提供され、第三者が市内交換会社の加入者に対して競合する電話関連サービスを提供することができる、という出来事である。言い換えれば、任意にせよ規制的な命令によってにせよ、市内交換会社（ＬＥＣ:local exchange carriers）（すなわち、市内電話サービス・プロバイダー）は、音声接続の設定および切断を含む、電話会社が提供する現代の特徴およびサービスを支配する高度インテリジェントネットワークへのアクセスを、他者に許さなければならなくなることが予想される。

現代のインテリジェント公衆電話ネットワークにおいても、基本的な発呼の設定、切断、および経路選択に用いる上記の信号パスと同じ信号パスが用いられて

、強化したカスタム発呼の特徴を提供し、ビリング装置の動作を制御して課金記録を保っている。従って、このネットワークに市内交換会社以外のものがアクセス

することを許すということは、危険を伴う計画である、ということが理解されよう。電話システムを制御するデジタルネットワークにアクセスしそのネットワーク内に記憶された情報にアクセスする者が不注意または悪意であれば、第三者へのアクセスが行われるときに適切な予防措置を講じない限り、公衆電話ネットワークの正しい動作がひどく妨げられたり、課金データを含むネットワーク内に記憶された情報が改ざんされたり、ネットワーク内に記憶された個人情報が不正に入手されたりする可能性がある。従って、本発明は、公衆電話システムのインテリジェントネットワークへのアクセスがオープンになることを見越してなされた。

本発明の必要性および本発明の実施の両方を理解するためには、まず最初に、現代の高度インテリジェントネットワークの基本アーキテクチャおよびインターフェースが第三者に提供される可能性があるという点を理解することが必要である。本明細書の図１は、典型的な市内交換会社のＡＩＮの少なくとも一部を示すブロック図である。このブロック図は簡単であるが、その構成要素は当業者にはよく知られている。典型的な公衆電話ネットワーク内には、複数の電話局交換機が設けられている。サービス交換点（ＳＳＰ: Service Switching Point）が、現代の電話局交換機のＡＩＮ構成要素である。これを、図１にＳＳＰ交換機１５－１５’として示す。１５と１５’の間の破線は、数が任意であることを示している。また、交換機１６等のＳＳＰでない交換機も、ネットワークに含まれている。

ＳＳＰ電話局交換機とＳＳＰでない電話局交換機の違いは、前者がインテリジェントネットワークの機能性を含んでいるということである。これは、その交換機が適当なハードウェアおよびソフトウェアを装備していて、１組の所定の状態が検出されると、交換機が加入者回線上の所定の発呼状態のトリガを開始し、ＡＩＮを介して送られるべき適切なメッセージとしてそのトリガを生成し、ネット

ワークからある行動をとるように命令する応答を受け取るまでは発呼の取扱を保留するようになっている、ということを示す。または、交換機は、タイムアウトが起こって交換機が行った照会に対してネットワークが何の返答もしない場合に実行する省略時タスクを有する。要するに、ＳＳＰ交換機とは、本明細書において説明する高度インテリジェントネットワークを扱い利用するように十分装備されたものである。

ＳＳＰでない交換機１６は、電子スイッチであって、ある基本パケット（rudimentary packets）を生成してネットワークを介して提供することができるが、かかる交換機に接続された加入者回線にインテリジェントネットワークで利用できるより複合的な特徴およびサービスを提供するためには、以下により詳細に説明する他の装置に依存せねばならない。電話局１５－１５’、１６はそれぞれ、一般に１７－１７’で示す、接続された複数の加入者回線を有する。通常、加入者回線の数は、１０，０００から７０，０００回線程度である。加入者回線１７－１７’のそれぞれは、顧客の構内装置の終端部分に接続されている。この終端部分は、交換機のそれぞれについての同様の複数の電話機１８－１８’で示す。

電話局交換機１５、１６を接続しているのは、図１に１９ａ，１９ｂで示す複数の中継回線である。これらは、電話局を相互接続する音声パス中継回線であり、発呼が完了したときにはこれらを介して接続される。通常の都市の環境における電話局の中継回線は、図１が暗示するようなヒナギクの花をつなげた輪のような配列に制限されるものではない、ということが理解されるべきである。言い換えれば、通常のネットワークにおいて、中継回線は電話局交換機１５’と電話局交換機１６の間に存在する。従って、２つの電話局の間で市内発呼が行われる場合には、これらの電話局を直接中継する接続が存在ししかもその中継回線が話し中でない場合には、ネットワークはその中継回線をその特定の発呼の完了に割り当てる。この２つの電話局を直接中継する回線がなかったり、回線はあるがすべて話し中である場合には、発呼は発呼側の電話局から少なくとも１個の他の電話局への中継回線に沿い、それに続く中継回線の接続を通って被呼側の電話局へと経路が選択される。

この一般的なアーキテクチャは、多数の市内交換会社を含むより広範囲の地理的地域を考える場合に、拡大される。その場合には、重要な違いは、長距離中継回線のみを交換する相互交換会社の交換機(inter exchange carrier switches)が含まれている、ということだけである。

インテリジェント交換電話ネットワークのインテリジェンスの大部分は、図１に示す残りの構成要素にある。これらは、上述のオフィス間共通線信号体系の現在のバージョンを実施するコンピュータおよび交換機である。交換機１５ないし

１６のそれぞれは、それぞれデータリンク２１ａ、２１ｂ、および２１ｃを介して、市内（localの）信号中継点（ＳＴＰ: signal transfer point）２０に接続されている。現在これらのデータリンクは、信号方式７（ＳＳ７: Signaling System ７）と呼ばれる信号プロトコルを用いる、５６キロビット／秒の双方向性データリンクである。ＳＳ７というプロトコルは、当業者にはよく知られており、米国国家規格協会（ＡＮＳＩ: the American National Standards Institute）が公表している仕様書に説明されている。ＳＳ７というプロトコルは、層状プロトコルであり、それぞれの層がその上の各層にサービスを提供し、それぞれの層にサービスを提供するのにその下の各層に依存している。ＳＳ７プロトコルはデータパケットを用いる。データパケットは、パケット、情報パケット、メッセージパケット、またはメッセージと呼ばれることもあるが、どれも同じものを指す。データパケットは、通常の初めおよび終わりフラグおよびチェックビットを含む。さらに、可変長のユーザ固有のデータおよび経路選択ラベルを含む、信号情報フィールドが設けられている。メッセージの優先順位、メッセージの受信宛先の国内ネットワーク、およびメッセージを作り出したエンティティを識別するユーザ名、を識別するサービス情報オクテットが設けられている。また、パケット内には制御およびシーケンス番号も含まれており、その使用および受信宛先は当業者にはよく知られており、上に参照したＡＮＳＩ仕様書内に説明されている。

ＳＳ７プロトコルの主な特徴のひとつは、その層状の機能構成である。ＳＳ７プロトコルの転送機能は、４つのレベルに分けられる。そのうちの３つは、メッ

セージ中継部（ＭＴＰ：Message Transfer Part）を構成する。４つ目のレベルは、共通の(common)信号接続制御部（ＳＣＣＰ：Signaling Connection Control Part）からなる。ＳＳ７プロトコルは、以下の４つの基本的なサブプロトコルからなる。メッセージ中継部（ＭＴＰ）、これは、信号点(Signaling points)間の信号メッセージの基本的な経路選択の機能を提供する。信号接続制御部（ＳＣＣＰ）、これは、信号点間の発呼の設定以外のメッセージの中継のためのさらなる経路選択および管理機能を提供する。統合ディジタル通信サービスユーザ部（ＩＳＵＰ：Integrated Services Digital Network）、これは、信号点間の発呼の設定の信号情報の中継に備える。そして、トランザクション性能アプリケーション部（Ｔ

ＣＡＰ：Transaction Capabilities Application Part）、これは、信号点間の回線に関係しない情報の中継に備える。

交換機からのＳＳ７データパケットは、すべて信号中継点（ＳＴＰ）２０に行く。当業者であれば、信号中継点２０は単に、ＳＳ７プロトコルの適切な層内の経路選択情報に応答しパケットをその意図する受信宛先に送るようにプログラムされている単なる多ポート高速パケット交換機である、ということがわかるであろう。信号中継点は、通常、それ自体パケットの受信宛先ではなく、単に、データパケットを生成しデータパケットに応答するネットワーク上の他のエンティティの間の呼量を管理する。ＳＴＰ２０等の信号中継点装置が従来ネットワーク内に冗長なペアを組んで設備されており、１個の装置が故障しても、最初のＳＴＰがサービスに戻ることができるまでそれとペアになっているもう片方が引き継ぐようになっていることに注意するべきである。実際は、信頼性をさらに高めるために、電話局交換機１５ないし１６のそれぞれの間に冗長データリンクがある。図面を簡単にするために、冗長装置は本明細書の図面には示していない。

信号中継点２０には、ＳＳ７データリンク２５を介して、１ＡＥＳＳのネットワークアクセスポイント（ＮＡＰ：network access point）２２も接続されている。ネットワークアクセスポイント２２は、トリガの状態を検出するようにプログラムされた計算装置であり、ＡＩＮのネットワークシステムにこれらのトリガ

が検出されたことを告知するのに、ＳＳＰ交換機のサポートを必要とする。１個のＳＳＰで多数のＮＡＰ交換機をサポートすることができる。論理的に、このＳＳＰは、もしＳＳＰを装備した交換機であったならば１ＡＥＳＳのＮＡＰに送られるネットワークが生成するパケットの多くの、受信宛先として指定されている。

情報の大半、およびネットワークの新しい強化した特徴の多くの基礎は、ＳＳ７データリンク２７を介して信号中継点２０に接続された市内サービス制御点（ＳＣＰ：service control point）２６にある。当業者には知られているように、サービス制御点は、比較的パワフルな故障を許容するコンピュータによって、物理的に実施される。典型的な実施装置は、どちらも米国電話電信会社販売の、スターサーバー(Star Server)ＦＴモデル３２００、またはスターサーバーＦＴモデル３３００を含む。これらのコンピュータのアーキテクチャは、それぞれタンデ

ム社のインテグリティ(Integrity)Ｓ２およびインテグリティＳ１のプラットフォームをベースにしている。公衆電話ネットワークの大部分の実施においては、信頼性およびネットワークが続いて動作することを確実にするために、サービス制御点も冗長に接続したペアを組んで設けられている。

サービス制御点を実施する計算装置は、通常、１個のドライブにつき３００メガバイトから１．２ギガバイトの範囲のディスクドライブを１個から２７個収容でき、２４から１９２メガバイト程度のメインメモリを有する。従って、これらが大型でパワフルな計算マシンであるということが理解されよう。サービス制御点が果たす各機能の中に、強化したサービスを提供するのに用いるネットワークのデータベースの維持がある。ＳＣＰを実施するコンピュータは、１秒あたり１７００万個程度の速度で命令を実行することができる。ＳＳ７プロトコルを用いると、これは１秒あたり約５０から１００個のネットワークのメッセージのトランザクション（照会／応答のペア）になる。

サービス制御点のコンピュータは最初、８００番サービス、すなわちフリーダイヤル（発呼者にとって）の長距離サービスの実施に必要なトランザクションお

よび課金トランザクションを取り扱うためにネットワークに導入された。８００番の加入者は、その加入者の８００番の番号に通話が申し込まれると発呼される少なくとも１個のダイヤル呼び出し方式の回線の番号を有している。この８００番の市外局番に対応する物理的な電話局や国の地域はない。多くの電話局交換機でその度に変換情報を提供するよりも、８００番通話の加入者電話番号の索引を作ることができる中心位置(central locations)をいくつか設ける方がかなり経済的である。現在、サービス制御点は、クレジットカード通話のトランザクションのデータベースも含む。

また、サービス制御点は、ある特定のサービスの顧客を識別するデータベースも含む。交換機１５－１５’等の交換機におけるデータおよび発呼の処理をできる限り簡単で一般的なものにしておくために、それぞれの発呼について交換機において比較的小さな組のトリガが規定されている。このネットワークにおけるトリガは、サービス制御点に送られるパケットを生成するある特定の加入者回線と関連する現象である。このトリガによって、サービス制御点はそのデータベース

に照会を行い、この特定の発呼について何らかのカスタム化した発呼の特徴または強化したサービスを実施するべきか、あるいはその発呼に従来の普通のダイヤル呼び出し方式の電話サービスを提供するべきかを決定する。データベースの照会の結果は、ＳＣＰ２６からＳＴＰ２０を通って交換機に送り戻される。

戻りパケットは、その発呼の処理方法に関する交換機への命令を含む。この命令は、カスタム化した発呼サービスまたは強化した特徴の結果として何か特別な行動を取ることもよいし、あるいは単に、その特定の発呼に何か普通の電話サービス以外のものを提供するべきだということを示す入力がそのデータベースにないということを示すものでもよい。後者のタイプのメッセージを受け取る場合、これに応答して、交換機はその発呼状態を通過し、被呼ディジットを集め、その発呼を設定しその経路を選択するのに用いられるさらなるパケットを生成する。これについては上に説明したとおりである。

様々な市内交換会社の中で発呼の経路を選択する同様の装置が、地域信号中継点２８および地域サービス制御点２９において設けられている。地域ＳＴＰ２８

は、ＳＳ７データリンク３０を経由して市内ＳＴＰ２０に接続されている。地域ＳＴＰ２８は、対応する市内装置間のデータリンク２７と物理的にも機能的にも同じデータリンク３１を経由して、地域ＳＣＰ２９と接続されている。市内装置と同様、信頼性を高くするために、地域ＳＴＰおよびＳＴＣは冗長に接続したペアを組んで設けられている。

市内および地域のサービス制御点２６、２９の両方が、それぞれのデータリンク３５、３６を経由して、サービス管理システム（ＳＭＳ:service management system）３７に接続されている。このサービス管理システムもまた、大型の汎用デジタルコンピュータおよび市内交換会社および相互交換会社の事務所へのインターフェースによって実施されている。サービス管理システムは、加入者がそのＡＩＮサービスを全体的に変更する場合にサービス制御点２６、２９のデータベースに情報をダウンロードする。同様に、サービス管理システムは、リアルタイムでないベースで、電話会社の加入者に提供したサービスのインボイスを適切に作るために必要な課金情報をダウンロードする。

現代の高度インテリジェントネットワークはまた、図１に示すサービス接続点

３９等のサービス接続点（ＳＮ: service node）も含む。当業者であれば、サービス接続点には精通しており、サービス接続点は物理的にはサービス制御点２６、２９を実施するのと同じタイプのコンピュータによって実施される。サービス接続点３９は、計算性能がありデータベースを維持するという特徴に加え、音声およびＤＴＭＦ信号認識装置、および音声合成装置も含む。サービス接続点３９は、データリンク４０を経由して、ＳＣＰ２６、２９にサービスを提供するのと略同じ方法でサービス接続点にサービスを提供するサービス管理システム３７に接続されている。サービス接続点３９は、物理的にはＳＣＰ２６と非常に似ているが、その使用においては、重要な違いがいくつかある。ＳＣＰ２６等サービス制御点は通常、発呼を送ったり８００番の変換や経路選択等の大量経路選択サービスを実施する。また、クレジットカード番号のバリデーション等の課金の承認のための大量データベースを維持しそれへのアクセスを提供するのにも用いられている。市内交換会社ネットワークの大部分において、サービス制御点は、発呼

の論理的完了、すなわち被呼加入者回線への呼び出し信号の供給および発呼加入者への呼び出しに先だって行われるデータベース検索および経路選択サービスにのみ用いられる。

これとは対照的に、サービス接続点３９等のサービス接続点は主に、発呼への音声接続、あるいは発呼の間またはその後に交換された接続を経由して加入者にかなりの量のデータの転送を必要とする何らかの強化した特徴またはサービスが必要な場合に用いられる。図１に示すように、サービス接続点３９は通常、４１で示す統合ディジタル通信サービス（ＩＳＤＮ：Intefrated Service Digital Network）リンクを経由して１個またはそれ以上の（しかし通常数個のみの）交換機に接続されている。したがって、発呼中に（すなわち、呼び出し信号の完了または被呼加入者のピックアップの後）実施されるサービスは通常、サービス接続点３９等のサービス接続点の設備を用いる。

読み手のために例を挙げると、発呼者の音声による告知は、サービス接続点３９を経由して実施されるカスタムの特徴である。ある加入者が別の加入者であるジョーンズさんの番号をダイヤルし、ジョーンズさんは入呼びの音声による告知を提供するサービスを契約していると仮定しよう。ＳＳＰを装備した交換機の発

呼進行状態のうちのひとつが、ダイヤルされたディジットを集めた後、交換機が成端要求トリガを生成するときに起こる。このトリガは、ＳＴＰ２０を通ってＳＣＰ２６へと経路選択されその特定の被呼者番号を識別するＳＳ７データパケットからなる。ＳＣＰは、記録を検索してジョーンズさんの電話回線と関連する加入者電話番号を探し、彼女が、入呼びを識別する音声による告知を提供するサービスの加入者であることを検出する。するとＳＣＰ２６は、パケットをデータリンク２７を介してＳＴＰ２０に送り戻し、パケットは発呼者の加入者回線と関連する電話局とジョーンズさんの加入者回線と関連する電話局の両方に送られる。

発呼者の電話局は、待機するかまたは発呼者の加入者回線に再度、折り返し呼び出しを行うように指示される。別のパケットが、交換機１５’に送られる。このパケットには、ジョーンズさんの加入者電話番号、発呼者の番号、およびサービス接続点３７における音声合成機のチャネルへのアクセスの要求、を含む。交

換機１５’は、ＩＳＤＮリンク４１を経由してサービス接続点と音声およびデータ回線を接続し、パケット（適切なＩＳＤＮのフォーマットの）をサービス接続点に通す。するとサービス接続点は、そのデータベースに照会を行って、ジョーンズさんの記録（実際には彼女の加入者電話番号の記録）にその特定の発呼番号の入力があるかどうかを決定する。

一方で、電話局１５’とジョーンズさんの電話回線を担当する電話局の間で、必要な音声中継回線が接続されており、従って、ジョーンズさんの加入者回線に応答監視信号が戻されるときには、サービス接続点３９における合成機とジョーンズさんの間には音声パスが存在している。すると合成機は、発呼者の識別を告知し、ジョーンズさんの電話に出ている人は、適切な行動（電話上のある特定の番号を押す、等）をとって、その電話に出たいかどうかを示すことができる。ＤＴＭＦ番号は、サービス接続点におけるＤＴＭＦ認識回線によって認識され、これも同様に、音声回線上に繋がれる。するとサービス接続点は、その発呼が受諾されたか拒絶されたかを示す適切なパケットを生成し、それらのパケットはＩＳＤＮリンク４１を経由して交換機１５’に進む。交換機において、プロトコルの変換が行われ、これらのパケット内の情報が適切なＳＳ７プロトコルのパケットにフォーマットされ、そして信号中継点２０に通され、適切な局に送られて、発呼者とジョーンズさんの加入者回線の間の音声リンクを設定するか、または適当な音響式確認（話中音やリオーダ音等）を発呼者に提供する。

前述の説明は、現在の公衆電話システムである高度インテリジェントネットワークの動作を、いくつか例を挙げて基本的に概観するものである。当業者にも、偶然本明細書を読んで興味を持った人にも明らかとなるとおり、ネットワークを通るデータパケットのインテグリティ（完全さ）は、ネットワークの動作にとってきわめて重大である。システムが正しく機能して発呼が完了するように、パケットのインテグリティは維持されねばならない。また、ＳＳ７データパケットが音声回線容量の割り当てを制御するので、ネットワークが正しく動作するためには、中継回線容量に対するスプリアス（偽の）の、つまり不要の要求がネットワーク内で生成されないことが決定的に重要である。

本発明の発明者は、ネットワークのＳＳ７データリンクを第三者にオープンにして、第三者が電話ネットワークを介してカスタム化したサービスを提供できるようにすることが、第三者のプロバイダーが提供するサービスの性質について市内交換会社に広範な情報を提供する必要がなくなるように規定される、と考えている。従って、ネットワークを、第三者である強化した発呼サービスの供給者にオープンにする見込みであるということは、市内交換会社のネットワークと第三者の間のインターフェースにおいて注意して取り次がねばならず、アクティビティおよびデータパケットのメッセージを監視してネットワークのインテグリティおよび動作、およびサービス・プロバイダーの加入者すべてのプライバシー、の両方を保護せねばならない、ということである。

また、ネットワーク内のデータベースに維持されている情報の多くは、市内交換会社（ＬＥＣ）の顧客の機密に関わる商業上の情報を構成する可能性がある。企業が電話を受ける度合い、企業が受ける８００番の呼量、あるいは特定の企業への電話の時間的特性さえも、ＬＥＣの顧客のライバルにとって有用かもしれない情報を構成する可能性がある。従って、ネットワークがオープンになる場合には、注意深くチェックしてＬＥＣの顧客以外の者がアクセスできる情報のタイプを制限する必要がある。

発呼の経路選択を制御する別個のＳＳ７の信号パケットを現在使用するように

なったのは、かなりの部分、カスタム発呼サービスまたは強化したサービスを提供するために発呼の経路を変更する必要があったからである。この最も簡単な例は、もちろん、１本の加入者回線向けに意図された発呼を別の１本に転送する、ということである。しかし、発呼の経路を変更してダイヤルされた番号と関連するもの以外の加入者回線に送ることができるということはまた、ネットワークが第三者であるデータパケットのジェネレータにオープンになったときには、潜在的な商業上の悪影響にも通じるものである。

例えば、重要な新顧客源として入電話を用いている企業のライバルは、野放しにされていれば、サービス制御点のコンピュータに、そのネットワークのメッセージを生成した企業の電話にライバルから電話を転送するように命令するパケッ

トをネットワーク上に生成することができる。これを定期的に行って、転送命令を短期間だけ適当な位置になるようにし、ある割合の入呼びをこのような方法で抜き取ることができる。従って、ネットワークが第三者にオープンになる場合には、承認されていないまたは不適切な、発呼の経路変更や発呼への干渉を行おうとする試みから、発呼の経路選択の処理のインテグリティを保護し、ネットワークにアクセスできる第三者の存在が影響を与えないようにすることが必要である。

要約すると、高度インテリジェントネットワークは、電話の通話の取り扱いに多くの用途を開く、複合的高速高呼量パケット交換のメッセージを送る方法である。大部分のネットワーク要素は、そして特にＳＳＰ交換機は、ある事象があると比較的簡単なフォーマットの照会メッセージが生成され、発呼の処理を続行する前にネットワークからの応答を待つように設計されている。これらの手順には、照会に対する応答が受け取られない場合にはタイムアウトするウォッチドッグタイマが用いられる。しかし、さらなる発呼の進行が、有効な応答と対比されるタイムアウトが起こることにより制御される状況では、処理している発呼のうちのかなりの割合について、ネットワークの性能がかなり劣化する。そうすると、顧客は発呼処理で過度に遅れたり、強化した特徴の提供を適切に受けることができない、ということを経験することになる。本質的に、ネットワークを多用途に使えるようにすると、そのネットワークは不適切なネットワークのメッセージに対して脆弱になる。従って、ネットワークをオープンにして、第三者である強化し

たサービス・プロバイダーに高度インテリジェントネットワークへのアクセスができるようにすると、市内交換会社と第三者であるサービス・プロバイダーの間のインターフェースを通るメッセージの呼量の取り次ぎを行い、第三者であるサービス・プロバイダー側のインターフェースでの悪影響、人的エラー、および装置の故障からネットワークを保護する必要がある。

発明の概要

本発明は、ＳＳ７プロトコルのオープンなアクセス環境においてネットワーク

要素の使用によりオープンな高度インテリジェントネットワーク環境における高度インテリジェントネットワークのメッセージの呼量を取り次ぐ方法である。より詳細には、本発明の好適な形態は、多数のサービス・プロバイダーのサービスに関する命令を供給するサービス・プロバイダーのＳＣＰから受け取られたまたはそこへ向かうデータパケットに関して、ＳＴＰにおいておよび取り次ぎアクセス(mediated access)ＳＣＰにおいて取り次ぎ手順を用いることによって、高度インテリジェントネットワークにおいて達成される。

高度インテリジェントネットワークを、市内交換会社でないサービス・プロバイダーにオープンにすることによって、一方で、システム内のすべての要素に、高度インテリジェントネットワークのメッセージの受信宛先および応答の適切な受信宛先を明白に検出させる必要性と、他方で、サービス・プロバイダーが高度インテリジェントネットワークへのアクセスを悪用してライバルに関する情報に不適切なアクセスをしたり、どうにかしてネットワークの動作やシステム上のある特定のライバルのアプリケーションの動作を妨害する、ということができないように保証する必要性との間に、緊張関係が作り出される。

高度インテリジェントネットワークへの承認されていないアクセスを防止するために、本発明は、ＳＴＰにおけるゲートウェイ・スクリーニングを用いて、サービス・プロバイダーのＳＣＰ等の市内交換会社のものでないネットワーク要素から発信されたデータパケットに関してある取り次ぎ手順を行う。ＳＴＰは、データパケットに、妥当な発信コード、妥当な受信宛先コード、妥当なサービスインジケータがあるかチェックする。また、他に選択されたパラメータの妥当性があるかチェックしてもよい。これらの値のうちのいずれかが無効であれば、データパケットは拒絶される。これらの値が妥当であれば、ＳＴＰはデータパケットを取り次ぎアクセスＳＣＰに送信する。

高度インテリジェントネットワークへの承認されていないアクセスをさらに防止するために、本発明は、取り次ぎアクセスＳＣＰを用いて、サービス・プロバイダーのＳＣＰ宛のデータパケットから、ある情報を除去する。この情報が除去されるのは、サービス・プロバイダーがその情報を用いてネットワークやネット

ワーク上で実行されているアプリケーションに関する不適切な情報を得ることがないようにするためである。ネットワークを通るデータパケットの経路選択を妨げることなくこの情報の除去を行うために、本発明は、取り次ぎアクセスＳＣＰがその情報を代用情報と取り替える、ということを規定している。特に、取り次ぎアクセスＳＣＰは、データパケットを発信したネットワーク要素によって割り当てられたトランザクション番号、発信ネットワーク要素に対応する発信点コード、および発信ネットワーク要素のサブシステム番号、に対応するデータパケット内の情報を除去する。好ましくは、第１のトランザクション番号、発信点コード、およびサブシステム番号は、データパケットの第１のトランザクション識別子を含む。第１のトランザクション識別子は、取り次ぎアクセスＳＣＰによって記憶される。除去された情報の代用物として、取り次ぎアクセスＳＣＰは、第２のトランザクション番号と呼ばれる乱数を生成する。これは、取り次ぎアクセスＳＣＰとサービス・プロバイダーのＳＣＰの間の信号経路において用いられるデータパケットと関連する。第２のトランザクション番号として乱数を用いることにより、データパケットの受領者にはネットワークの動作に関する情報が一切供給されない。取り次ぎアクセスＳＣＰは、第２のトランザクション番号を記憶し、特に、記憶された第２のトランザクション番号は、記憶された第１のトランザクション識別子に写像される。好ましくは、取り次ぎアクセスＳＣＰはまた、第２のトランザクション番号のあるデータパケットの受信宛先点コードを記憶する。

高度インテリジェントネットワークへの承認されていないアクセスを防止する他の方法として、本発明は、取り次ぎアクセスＳＣＰを用いて、応答として受け取られるデータパケットの妥当性を検査する。妥当な応答については、データパケットは、元々取り次ぎアクセスＳＣＰ２６’によってデータパケットに割り当てられた第２のトランザクション番号を含むべきである。データパケットがこの第２のトランザクション番号を含まない場合には、そのデータパケットは拒絶される。好ましくは、サービス・プロバイダーのＳＣＰから受け取った応答に関して、取り次ぎアクセスＳＣＰは、受け取ったトランザクション番号およびサービ

ス・プロバイダーのＳＣＰのＳＳ７の発信アドレス（または点コード）を、第２のトランザクション番号および照会であったときのデータパケットの受信宛先点コードと比較する。比較したトランザクション番号と点コードは合わねばならず、そうでない場合にはデータパケットは拒絶される。この第２の比較は、サービス・プロバイダーの応答の経路が故意でなく直接ＳＳＰへと選択されることの悪用から保護し、「不正な」ＳＳ７プロトコルの回線から保護する。受け取られた情報が記憶されている情報に対応する場合には、取り次ぎアクセスＳＣＰは、記憶装置から対応する第１のトランザクション識別子を取得する。第１のトランザクション識別子は、取り次ぎアクセスＳＣＰに、データパケットのさらなる経路選択または受信宛先情報を供給する。

本発明はまた、取り次ぎアクセスＳＣＰがサービスするサービス・プロバイダーのＳＣＰの状態の監視において取り次ぎアクセスＳＣＰが達成する各手順によって高度インテリジェントネットワークを管理する方法を提供する。管理方法の１態様において、取り次ぎアクセスＳＣＰは、サービス・プロバイダーのＳＣＰが応答メッセージを戻すのにかかる時間の経過を追う。サービス・プロバイダーのＳＣＰが応答メッセージを戻すのに、指定した最小時間よりも長く時間がかかる場合には、取り次ぎアクセスＳＣＰは、照会メッセージを取り次ぎアクセスＳＣＰに与えられたときに廃棄する（拒絶する、とも呼ばれる）ことによって、サービス・プロバイダーの新しいメッセージの負荷を減らす手段を講じる。本発明の管理方法の他の１態様は、取り次ぎアクセスＳＣＰが、以前にアウトオブサービスであると決定されたサービス・プロバイダーのＳＣＰの状態を監視する、ということである。好ましくは、取り次ぎアクセスＳＣＰは、定期的にアウトオブサービスのサービス・プロバイダーのＳＣＰにテストメッセージを送る。１つのテストメッセージ、または一連のテストメッセージがサービス・プロバイダーの

ＳＣＰによって正しく取り扱われる場合には、サービス・プロバイダーのＳＣＰへの呼量は、取り次ぎアクセスＳＣＰによって自動的に再開される。

従って、本発明の目的は、市内交換会社だけでなく、高度インテリジェントネットワークにアクセスするサービス・プロバイダーにとって、およびサービス・

プロバイダーの顧客にとって、高度インテリジェントネットワークのプライバシー、セキュリティー、および信頼性を提供することである。

また、本発明の目的は、高度インテリジェントネットワークにおいてデータパケットの呼量を取り次ぐ改良した方法を提供することである。

本発明がこれらの目的を達成し、オープンな高度インテリジェントネットワーク環境における市内交換会社の必要を満たす、ということは、以下の好適な実施例の詳細な説明から理解されるであろう。

図面の簡単な説明

図１は、それを制御する高度インテリジェントネットワークを含む、従来技術の現在の交換電話ネットワークの図である。

図２は、本発明の好適な実施例を実施する装置のブロック図である。

図３は、好適な実施例による要素間のデータパケットの流れのフローチャートである。

図４は、好適な実施例により信号中継点が行う取り次ぎ手順を示すフローチャートである。

図５は、好適な実施例により取り次ぎアクセスサービス制御点が受け取るデータパケットの取り扱いを示すフローチャートである。

図６は、好適な実施例により取り次ぎアクセスサービス制御点が行う取り次ぎ手順を示すフローチャートである。

図７は、好適な実施例により取り次ぎアクセスサービス制御点がサービスするサービス・プロバイダーのサービス制御点の状態を監視する管理方法を示すフローチャートである。

図８は、好適な実施例によるメッセージの流量の監視および管理を示すフローチャートである。

好適な実施例の詳細な説明

次に図面に移って、本発明の好適な実施例を説明する。図面では、同じ番号は同じ部品および手順を指す。図２は、好適な実施例を実施する装置のブロック図を示し、上の「発明の背景」に関連して説明した図１に示す典型的なＡＩＮのネ

ットワーク要素の一部を示す。

特に、図２は、２個のサービス交換点（ＳＳＰ）１５、１５’が、関連する交換機を中継回線１９ｂで相互接続して示されている。これらの交換機におけるＳＳＰの論理ノードのそれぞれは、それぞれＳＳ７データリンク２１ａ、２１ｂによって、信号中継点（ＳＴＰ）２０’に接続されている。好ましくは、そして今では信頼性の目的のために普通であるが、ＳＴＰはペアを組んで配置されている。従って、ＳＴＰ２０’は、信頼性の目的のために、自らのＳＳ７データリンクの組を有するそれぞれのＳＴＰとのペアとして配置されている。しかし、図を簡単にするために、ＳＴＰのペアのうちの１つのみ、およびＳＳ７データリンクのうちの１組のみを図２に示す。図２において、ダッシュをつけて示して参照する番号は、前に紹介した同等物と非常に似た装置を指すが、本発明を実施するのに用いられる目的のためにある機能性が付け加えられている。図２において、本発明を実施するために、以下に図３、図４に関して説明するあるゲートウェイ・スクリーニング機能がＳＴＰ２０’に付け加えられている。「ゲートウェイ」とは、通信ネットワークへの入口およびそこからの出口である。図２において、ＳＴＰ２０’は、サービス・プロバイダーのサービス制御点（ＳＣＰ）４７を通るサービス・プロバイダーにとって、図１に示すような高度インテリジェントネットワーク（ＡＩＮ）へのゲートウェイである。

ＳＴＰ２０’は、ＳＳ７データリンク２７を経由して、市内交換会社（ＬＥＣ）が動作する取り次ぎアクセスサービス制御点（ＳＣＰ）２６’に接続されている。ＳＴＰ２０’に関しては、取り次ぎアクセスＳＣＰ２６’は、好ましくは、信頼性の目的のために、それぞれのペアが自らのＳＳ７データリンクの組を有するＳＣＰのペアとして配置されている。しかし、図を簡単にするために、ＳＣＰのペアのうちの１つのみ、およびＳＳ７データリンクのうちの１組のみを図２に示す。取り次ぎアクセスＳＣＰ２６’は、物理的に、図１に示すＳＣＰ２６と同じであ

り、従って、コンピュータを有する。しかし、取り次ぎアクセスＳＣＰ２６’のコンピュータは、図３、図５、および図６に関して以下に説明する好適な実施例

のある各手順を実行するためのプログラム命令を含む。取り次ぎアクセスＳＣＰ２６’のコンピュータ（別個には示していない）はまた、従来技術と同様の顧客の記録を含み、本発明を達成するためのサービス・プロバイダーの記録を含む、データベース４５も有する。

ＳＴＰ２０’は、別のＳＳ７データリンク４６を経由して、サービス・プロバイダーのＳＣＰ４７に接続されている。一般的に、サービス・プロバイダーのＳＣＰ４７は、何らかの交換式電話による通信サービスの形式を供給するいかなるエンティティが動作してもよい。もっとも、サービス・プロバイダーのＳＣＰ４７は、そのネットワークを図１に示す市内交換会社以外のエンティティが動作するＳＣＰを表すことが多い。図２はさらに、サービス・プロバイダーのＳＣＰ４７と現在のＡＩＮの間のインターフェースを、ＳＳ７データリンク４６に添った点４８として示す。

図２に示す実施例は、以下に説明する図３ないし図５に示す各手順を実行する。高度インテリジェントネットワークのメッセージを含むデータパケットの流れを図２に関して説明し、取り次ぎ処理における各手順を図３ないし図６に関して詳細に説明する。図２の実施例における取り次ぎは、ＳＴＰ２０’のゲートウェイ・スクリーニング機能においてと取り次ぎアクセスＳＣＰ２６’においての両方で起こる。

一般に、図２に示す本発明の実施例において、データパケットの流れの経路は以下の２つがある。（１）ＳＳＰ１５－１５’から、ＳＴＰ２０’、取り次ぎアクセスＳＣＰ２６’、ＳＴＰ２０’、そしてサービス・プロバイダーのＳＣＰ４７へ、および（２）サービス・プロバイダーのＳＣＰ４７から、ＳＴＰ２０’、取り次ぎアクセスＳＣＰ２６’、ＳＴＰ２０’、そしてＳＳＰ１５－１５’へ。

一般的に、発呼に関係するデータパケットは、最初第１の流れの経路をたどり、サービス・プロバイダーのＳＣＰ４７において応答が得られると、発呼に関係するデータパケットは次に第２の流れの経路をたどる。他方で、一般的に、発呼に関係しないデータパケットは、最初第２の経路をたどり、高度インテリジェント

ネットワーク要素から応答が得られると、発呼に関係しないデータパケットは次に第１の流れの経路をたどる。データパケットが発呼に関係するデータパケットにせよ発呼に関係しないデータパケットにせよ、データパケットの発信点（図２において、ＳＳＰ１５－１５’またはサービス・プロバイダーのＳＣＰ４７）が、流れの経路においてデータパケットが出会う取り次ぎ手順の組を決定する。一般的に、サービス・プロバイダーのＳＣＰ４７等の市内交換会社でない発信源から発信されるデータパケットは、ＳＴＰ２０’において主な１組の取り次ぎ手順に、そして取り次ぎアクセスＳＣＰ２６’において他の主な１組の取り次ぎ手順に出会う。データパケットは他の点においても取り次ぎ手順に出会う可能性があるが、かかる取り次ぎは本明細書に説明する取り次ぎ手順と比較して含む手順が少ない、ということに注意するべきである。例えば、ＳＳＰ１５－１５’は、ＡＩＮの入メッセージのプロトコル構造を妥当とする取り次ぎ手順を含む可能性がある。しかし、ＳＳＰ１５－１５’等のネットワーク要素から発信されるデータパケットは、取り次ぎアクセスＳＣＰ２６’においてのみ主な１組の取り次ぎ手順に出会う。ネットワーク要素から発信されるデータパケットが主な１組の取り次ぎ手順にのみ出会うのは、データパケットのネットワーク発信点が高度インテリジェントネットワークのインテグリティに関して安全であると感知され、それによってＳＴＰ２０’におけるさらなる取り次ぎが不要になるからである。

さらに図２を参照して、発呼に関係するデータパケットの一例を参照してこの２つの流れの経路を示す。データパケットの第１の流れの経路の創設は、ＳＣＰ４７と関連するサービス・プロバイダーを前もって選択しておりその加入者回線がＳＳＰ１５に接続されている顧客が、自分の電話を取ってオフフックにするときに始まる。ＳＳＰ１５は、それに応答してトリガを生成する。このトリガは、ある特定の加入者電話番号と関連する電話がオフフックになったということを示すメッセージを含む高度インテリジェントネットワークのデータパケットである。このデータパケットは、ＳＳＰ１５からＳＳ７データリンク２１ａを渡ってＳＴＰ２０’に通される。ＳＴＰ２０’は、データパケットの経路を、データリンク２７を渡って取り次ぎアクセスＳＣＰ２６’へと選択する。取り次ぎアクセスＳＣＰ２６’がこのデータパケットを受け取ると、１組の取り次ぎ手順が行われ

る。

これらの手順は、図３、図５、および図６に関して以下に説明する。取り次ぎが成功した場合には、取り次ぎアクセスＳＣＰ２６’はさらに、データパケットの経路をＳＳ７データリンク２７を渡ってＳＴＰ２０’へと選択する。その後このデータパケットは、ＳＴＰ２０’によって、ＳＳ７データリンク４６を渡ってサービス・プロバイダーのＳＣＰ４７へと転送される。

第２の流れの経路の創設は、サービス・プロバイダーのＳＣＰ４７が、取り次ぎアクセスＳＣＰ２６’から受け取ったデータパケットに応答してデータパケットを生成するときに始まる。この応答データパケットは、ＳＳＰ１５宛であり、発呼の処理において次にとるべき適切な行動に関する情報を含む。たいていの場合、次の手順は、顧客に発信音を供給するということである。サービス・プロバイダーのＳＣＰ４７は、データリンク４６を渡ってＳＴＰ２０’に応答データパケットを送る。サービス・プロバイダーのＳＣＰ４７からのデータパケットが受け取られると、ＳＴＰ２０’は、１組の取り次ぎ手順を行う。これらの取り次ぎ手順は、図３および図４に関して以下に説明する。取り次ぎが成功した場合には、ＳＴＰ２０’は応答データパケットをＳＳ７データリンク２７を渡って取り次ぎアクセスＳＣＰ２６’に送る。応答データパケットは再び、取り次ぎアクセスＳＣＰ２６’において１組の取り次ぎ手順に出会う。これらの取り次ぎ手順は、図３、図５、および図６に関して以下に説明する。この取り次ぎが成功した場合には、取り次ぎアクセスＳＣＰ２６’は、応答データパケットをＳＳ７データリンク２７を渡ってＳＴＰ２０’に送り、ＳＴＰ２０’は今度は、応答データパケットをＳＳ７データリンク２１ａを渡ってＳＳＰ１５に送り、さらなる発呼処理が行われる。

図３および図４に関してより詳細に説明するように、ＳＴＰ２０’がインターフェース４８を横切るデータパケットを受け取ることをやめたり、サービス・プロバイダーのＳＣＰ４７が適切な応答データパケットを生成することをやめるという状況が起こる可能性がある。本発明は、ネットワークがサービス・プロバイダーのＳＣＰ４７と効果的に通信することができない場合には、デフォルト（ｄ

ｅｆａｕｌｔ）・アプリケーションを適用する。かかるデフォルト・アプリケーションがない場合には、ＳＳＰ１５－１５’はそれらの内部のデフォルト・アプリケーションに完全に依存し、ＳＳＰ１５－１５’は、それぞれのＳＳＰと共に動作する内部のタイマのタイムアウトに応答してのみそれらのアプリケーションに進む。これらのタイマは、前に送信された出メッセージへの応答をＳＳＰが待つ時間の量を制限する。

当業者には、デフォルト・アプリケーションの選択の範囲が広いことが明白であろう。しかし、最も普通のデフォルト・アプリケーションは、電話サービス（ＰＯＴＳ：plain old telephone service）を設けることであろう。１実施例において、本発明は、サービス・プロバイダーが異なるデフォルトの応答を選択していない限り、すべての廃棄された最初の照会は応答メッセージの切断という結果になる、ということを規定する。オプションで、本発明は、すべての廃棄された最初の照会には取り次ぎアクセスＳＣＰ２６’からの選択されたデフォルトの応答が与えられる、ということを規定する。この特定のデフォルトの応答は、発信トリガのため等の発呼処理の継続であってもよく、成端試みトリガ(terminating attempt triggers)のため等の発呼の接続であってもよく、告知を用いることであってもよく、または発呼の切断であってもよい。さらに、選択されたデフォルトの応答は、トリガ／加入者電話番号をベースにして割り当てることができてもよい。ＳＳＰ１５－１５’からのデータパケットに適切な命令で応答するデフォルト・アプリケーションを設けることによって、高度インテリジェントネットワークを用いている発呼者がサービス・プロバイダーの側のインターフェース４８の装置の故障や悪用に弱い程度がかなり低くなる。

以下の本発明の方法のフローチャートの説明に関しては、図２を参照する。

図３は、データパケットがサービス・プロバイダーのＳＣＰ４７において発信されるにせよＳＳＰ１５－１５’等のネットワーク要素において発信されるにせよ、本発明の方法を示すフローチャートである。背景として、処理においてネットワーク要素間でのデータパケットの流れは、その流れが照会と関連する応答メッセージを１つよりも多く含んでいる場合には、会話型メッセージ・シーケンス

と呼ばれる。会話型メッセージでは、メッセージ・シーケンス（データパケット）が発呼処理において要素間を行ったり来たりして通る。メッセージ・シーケンスにおけるデータパケットは、すべてトランザクション性能アプリケーション部

（ＴＣＡＰ）のメッセージである。ＴＣＡＰメッセージは、信号点間の回線と関係しない情報の中継に備えるＳＳ７のサブプロトコルである。当業者には知られているように、メッセージ・シーケンスの第１のメッセージは、ＳＳ７プロトコルにおいて、照会または照会メッセージと呼ばれている。ＳＳＰ１５－１５’等のＳＳＰが生成するトリガは、照会の最も普通の形式である。しかし照会は、サービス・プロバイダーのＳＣＰ４７等のサービス・プロバイダーのＳＣＰによって生成されてもよい。一般的に、サービス・プロバイダーのＳＣＰは、発呼に関係しないメッセージの場面においてのみ照会を生成する。かかる発呼に関係しないメッセージは、自動呼び出しギャップ、更新要求、変化の監視のメッセージ、およびＳＣＰからＳＣＰへの照会／応答メッセージを含んでもよい。

本発明において、図３のステップ１００に示すように、照会を発信する要素は、照会に第１のトランザクション番号を割り当てる。トランザクション番号は高度インテリジェントネットワークにおいて既に用いられており、特に、一般的にＳＳＰによって生成されてある特定のＳＳＰトランザクションを識別する。第１のトランザクション番号はその発信要素にとって単一のものであるが、その番号は、高度インテリジェントネットワークの全体にわたって他の要素が生成する他のトランザクション番号と同一である可能性がある。従って、サービス制御点は、異なるＳＳＰから発信されるが同一の第１のトランザクション番号を有するメッセージ・シーケンスを取り扱う可能性がある。しかし、図５に関して以下に説明するように、サービス制御点は、ＳＳＰから受け取った第１のトランザクション番号をそのＳＳＰの発信点コード等の他の情報と連結することによって、メッセージ・シーケンスを識別する。

上で触れたように、照会は、発呼に関係しないメッセージの場面においてサービス・プロバイダーのＳＣＰによって生成される可能性もある。本発明において、サービス・プロバイダーのＳＣＰ４７は、現在用いられていない乱数（または

疑似乱数）を照会に割り当てることによって、第１のトランザクション番号をその照会に割り当てる。

再び図３を参照して、第１のトランザクション番号が発信要素によって生成された後、ステップ１０２で、第１のトランザクション番号と関連するデータパケットが、ＳＴＰ２０’等のＳＴＰに通されて受け取られる。図２を参照して、このデータパケットがサービス・プロバイダーのＳＣＰ４７から発信されている場合には、このデータパケットはＳＳ７データリンク４６を渡ってＳＴＰ２０’に通される。このデータパケットがＳＳＰ１５－１５’から発信されている場合には、このデータパケットはそれぞれＳＳ７データリンク２１ａまたは２１ｂを渡って通される。ステップ１０４で、ＳＴＰ２０’は、データパケットに関する取り次ぎが行われねばならないかどうかを決定する。上で触れたように、ＳＳＰ１５－１５’等の高度インテリジェントネットワーク要素において発信されるデータパケットは、高度インテリジェントネットワークのインテグリティに関して安全であると知覚されるので、ＳＴＰ２０’によって取り次がれない。従って、ＳＴＰ２０’が取り次ぎを行う必要がないと決定される場合には、本方法は、以下に説明するステップ１１４に進む。ＳＴＰ２０’が取り次ぎを行うと決定される場合には、ステップ１０６で、ＳＴＰ２０’がかかる取り次ぎを行う。ＳＴＰ２０’等のＳＴＰによる取り次ぎは、図４に関して以下に説明する。ステップ１０８で、データパケットがＳＴＰの取り次ぎを通ったかどうかが決定される。通っていない場合には、ステップ１１０で、そのデータパケットは拒絶され、メッセージの拒絶後点１１２でルーチンから抜ける。

データパケットがＳＴＰの取り次ぎを通っている場合には、ステップ１１４で、データパケットが取り次ぎアクセスＳＣＰ２６’に供給されるかどうかに関して決定がなされる。供給されない場合には、ステップ１１０でデータパケットは拒絶され、メッセージの拒絶後点１１２でルーチンから抜ける。データパケットが取り次ぎアクセスＳＣＰ２６’に供給される場合には、データパケットはＳＳ７データリンク２７を渡って取り次ぎアクセスＳＣＰ２６’に通され受け取られる。ステップ１１８で、取り次ぎアクセスＳＣＰ２６’は、このデータパケット

に関して取り次ぎを行う。この取り次ぎは、図５および図６に関してさらに説明する。取り次ぎの後、ステップ１２０で、このデータパケットが取り次ぎを通ったかどうかが決定される。通っていない場合には、ステップ１１０で、そのデータパケットは拒絶され、メッセージの拒絶後点１１２でルーチンから抜ける。図２に関して上で触れたように、好ましくは、本発明はデータパケットの拒絶に関してデ

フォルト・アプリケーションを備える。

データパケットが取り次ぎを通ると、ステップ１２２でデータパケットはＳＳ７データリンク２７を渡ってＳＴＰ２０’に通され、次にステップ１２４で、ＳＴＰ２０’がデータパケットを指定した受信宛先に通す。好ましくは、データパケットをサービス・プロバイダーのＳＣＰ４７に通す前に、取り次ぎアクセスＳＣＰ２６’が、サービス・プロバイダーのＳＣＰ４７またはデータパケットで要求された特定のサービス・プロバイダーのサービスが使用可能状態であるということを確認する。所望のサービス・プロバイダーのＳＣＰ４７または特定のサービス・プロバイダーのサービスがアウトオブサービスである場合には、取り次ぎアクセスＳＣＰ２６’はデータパケットを拒絶し、適用できる場合には、上に説明したデフォルト・アプリケーションを提供する。再び図２を参照して、データパケットの受信宛先がＳＳＰ１５－１５’である場合には、ＳＴＰ２０’はデータパケットをＳＳ７データリンク２１ａ－ｂのそれぞれを渡ってＳＳＰ１５－１５’に通す。受信宛先がサービス・プロバイダーのＳＣＰ４７である場合には、ＳＴＰ２０’はデータパケットをＳＳ７データリンク４６を渡って通す。ステップ１１２で、ルーチンから抜ける。

図４は、ステップ１０６の一部としてＳＴＰ２０’が行う好適な取り次ぎ手順を示すフローチャートである。上で触れたように、取り次ぎ手順は、データパケットがサービス・プロバイダーのＳＣＰ４７等の市内交換会社でないネットワーク要素から発信されている場合にのみ、ＳＴＰ２０’によって行われる。一般的に、ＳＴＰ２０’が行う取り次ぎ手順は、起点および受信宛先のＳＳ７プロトコルのアドレスの妥当性検査を含む。特に、本発明は、高度インテリジェントネッ

トワークでＳＴＰにおいて既に用いられているゲートウェイ・スクリーニング技術を用いることにより、ＳＴＰ２０’における取り次ぎを実施する。ゲートウェイ・スクリーニングにより、ＳＴＰは、データパケット内のアドレスおよびヘッダ情報の検査と、その検査した情報のＳＴＰが記憶している情報に関する比較をベースにして、受け取ったデータパケットを転送するかまたは拒絶する。当業者にはよく知られているように、ゲートウェイ・スクリーニングにおいて、ＳＴＰは一般的に、データパケットのフィールドまたはパラメータ内の以下のタイプの

情報の１つまたはそれ以上を検査する。すなわち、発信点コード、受信宛先点コード、およびグローバル名称アドレスである。データパケット内の情報をベースにして、ＳＴＰはデータパケットの経路を受信宛先情報に従って選択する。従って、従来技術においては、１つのデータパケットの経路選択の目的のために、ＳＴＰは多くの異なる受信宛先を受け入れていた。しかし、本発明においては、ＳＴＰは、１つのデータパケットの妥当な受信宛先として、割り当てられた取り次きアクセスＳＣＰを受け入れるのみである。本発明においては、ＳＴＰ２０’におけるゲートウェイ・スクリーニングを用いて、サービス・プロバイダーがデータパケットの経路を、サービス・プロバイダーのＳＣＰ４７からＳＴＰ２０’および取り次ぎアクセスＳＣＰ２６’を通るように選択するよう強制する。

図４は、好適な実施例において、ステップ１３２でＳＴＰ２０’が、データパケット内の第１のパラメータの妥当性をチェックすることによってデータパケットの送信者を識別することを示す。特に、ＳＴＰ２０’は、好ましくは、データパケット内の発信点コード（送信者識別子とも呼ぶ）がサービス・プロバイダーのＳＣＰ４７のポート識別子に対応するかどうかをチェックして、データパケットの承認されたプロバイダーからそのデータパケットが受け取られたことを確認する。言い換えれば、ＳＴＰ２０’は、インターフェース４８の物理的なポートの、ＳＳ７データリンク４６上のＳＣＰを動作することが承認されている特定のサービス・プロバイダーとの組み合わせの記録を記憶する。送信者の識別子が受領者のポート上のデータパケットの承認されたプロバイダーと対応しない場合には、そのデータパケットは１つのエンティティから発信されたことを表している

が、そのデータパケットが通ってＡＩＮに入ろうとしているポートのためにそのエンティティによって生成されるべきではなかったので、ＳＴＰ２０’がデータパケットが高度インテリジェントネットワークに入ることを許すことは不適切である。従って、発信点コードが無効の場合には、ステップ１３４で、データパケットは拒絶され、ステップ１３６でルーチンから抜ける。

発信点コードが妥当な場合には、ステップ１３８でＳＴＰ２０’がデータパケット内の第２のパラメータの妥当性をチェックする。特に、ＳＴＰ２０’は、好ましくは、受信宛先点コード（受信宛先アドレスとも呼ばれる）を、送信者のア

イデンティティと照合する。受信宛先点コードつまり受信宛先アドレスが、サービス・プロバイダーのＳＣＰ４７が通信することが許されていないネットワーク要素のものである場合には、データパケットは拒絶される。特にＳＴＰ２０’は、好ましくは、受信宛先点コードが、ＳＴＰ２０’の点コードに、ＳＴＰ２０’の別名点コードに、または取り次ぎアクセスＳＣＰ２６’に対応するかどうかをチェックする。受信宛先点コードが無効の場合には、ステップ１３４でデータパケットは拒絶され、ステップ１３６でルーチンから抜ける。

受信宛先点コードが妥当な場合には、ステップ１４０でＳＴＰ２０’がデータパケット内の第３のパラメータの妥当性をチェックし、特に、好ましくは、サービスインジケータが妥当であるかどうかをチェックする。好適な実施例において、妥当なサービスインジケータは、メッセージ中継部（ＭＴＰ）、信号接続制御部（ＳＣＣＰ）、またはテストメッセージに対応する。さらに、サービスインジケータのパラメータ（またはフィールド）の法定値は、米国ニュージャージー州のベルコア(BellCore)が発行した「信号システム第７の仕様書」、第Ｔ１．１１１．４節、ＴＲ－ＮＷＴ－０００２４６、第２号、第Ｉ巻（１９９１年６月）に規定されている。

好適な実施例において、ステップ１４０におけるチェックの結果、サービスインジケータが信号接続制御部（ＳＣＣＰ）に対応すると決定された場合には、ステップ１４２で、ＳＴＰ２０’はあるさらなるパラメータの妥当性のチェックを継続する。特に、ＳＴＰ２０’は、発呼者アドレス、被呼者アドレス、およびグ

ローバル名称変換をチェックする。発呼者アドレスは、法定点コード、サービス・プロバイダーのＳＣＰ４７のサブシステム番号の組み合わせ、またはサービス・プロバイダーのＳＣＰ４７に割り当てられた加入者電話番号（ＤＮ：Directory Number）と対応せねばならない。被呼者アドレスに関して、経路選択が点コードをベースにしておりサブシステム番号が示されている場合には、点コードは取り次ぎアクセスＳＣＰ２６’のものでなければならず、サブシステム番号は取り次ぎアプリケーションプログラムのものでなければならない。グローバル名称変換が示されている場合には、被呼者アドレスのフィールド内の変換タイプは、高度インテリジェントネットワークのオープンアクセス変換のタイプでなければならない。さらに、ＳＴＰ２０’がグローバル名称変換を行う場合には、結果として得られる受信宛先点コードおよびサブシステム番号は、取り次ぎアクセスＳＣＰ２６’のものでなければならず、サブシステム番号は取り次ぎアプリケーションプログラムのものでなければならない。

さらに、必要な可能性のある何らかの交互の(alternate)経路選択のために、図４に示していない他のチェックの手順をＳＴＰ２０’が行ってもよい。当業者にはよく知られているように、これらの交互の経路選択の手順は、単にネットワーク内のある交換ノードか非動作であるかどうか、および交互のアドレス経路選択を用いる必要があるかどうか、を決定する処理を構成する。

図５は、取り次ぎアクセスＳＣＰ２６’の受け取ったデータパケットの取り扱いを示すフローチャートである。一般的に、取り次ぎアクセスＳＣＰ２６’の行う取り次ぎ手順は、取り次ぎアクセスＳＣＰ２６’が受け取るＳＳ７プロトコルのデータパケットの高度インテリジェントネットワーク部の検査を含む。ステップ１４８で、取り次ぎアクセスＳＣＰ２６’はデータパケットを受け取る。取り次ぎアクセスＳＣＰ２６’が受け取るデータパケットは、発呼に関係するデータパケットであってもよく、発呼に関係しないデータパケット、照会、応答メッセージ、または他の会話型メッセージであってもよい。さらに、データパケットは、サービス・プロバイダーのＳＣＰ４７等のサービス・プロバイダーから受け取ってもよく、ＳＳＰ１５－１５’等のネットワーク要素から受け取ってもよい。

データパケットを受け取った後、取り次ぎアクセスＳＣＰ２６’は、決定のステップ１５０を実行する。この手順で、取り次ぎアクセスＳＣＰ２６’は、データパケットが照会（照会メッセージとも呼ばれる）を含んでいるかどうか、すなわち、データパケットが新しいトランザクションまたはメッセージ・シーケンス内の第１のメッセージであるかどうか、を決定する。照会は、ＳＳＰ１５－１５’等の値とワーク要素から受け取ってもよく、サービス・プロバイダーのＳＣＰ４７等のサービス・プロバイダーのＳＣＰから受け取ってもよい。データパケットが照会を含んでいる場合、ステップ１５２で、取り次ぎアクセスＳＣＰ２６’は、データパケット内に含まれている情報を用いてそのデータベース４５内の情報を探索し、経路を選択して、さらに発呼の処理を行う。例えば、データパケットがＳＳＰ１５－１５’からの照会を含んでいる場合、ステップ１５２で、取り次ぎアクセスＳＣＰ２６’は、データパケット内の情報を用いて、メッセージ内で識別された加入者電話番号をトリガするためのトリガを取り扱うサービス・プロバイダーのＳＣＰを探索する。このトリガおよびトリガする加入者電話番号は、データパケットが経路選択されるサービス・プロバイダーを、単一に識別する。特に、データパケットがＳＳＰ１５－１５’等のネットワーク要素から受け取られる場合には、取り次がれるアクセスＳＣＰ２６’は、好ましくは、そのデータベース４５を用いてトリガする加入者電話番号／トリガのタイプのペアを、顧客が期待するサービスを供給するサービス・プロバイダーのＳＣＰのＳＳ７プロトコルのアドレスに写像することができねばならない。この不可欠な写像は、サービス・プロバイダーの照会を受け取る承認のチェックである。このチェックにより、サービス・プロバイダーはその顧客のためのみにデータパケットを受け取ることが保証され、それにより、すべての参加しているサービス・プロバイダーの顧客にプライバシーおよびセキュリティが保証される。従って、取り次ぎアクセスＳＣＰ２６’は、好ましくは、システム内で動作しているサービス・プロバイダーのＳＣＰのそれぞれについてのすべての顧客の加入者電話番号のデータベース４５内の情報、およびサービス・プロバイダーのＳＣＰのそれぞれがアクセスすることが承認されているネットワーク要素に関する情報、を維持する。照会

がＳＣＰから発信されている場合には、その照会の被呼者アドレスのフィールド内の加入者電話番号は、取り次ぎアクセスＳＣＰ２６’のデータベース４５への入力に合わねばならない。これによって、それぞれのサービス・プロバイダーは自身の顧客のみに影響を与える、ということが保証される。好適な実施例において、市内アクセスおよび転送領域（ＬＡＴＡ：local access and transport area）内経路選択が用いられる場合には、サービス・プロバイダーのＳＣＰのアドレスは、メッセージ中継部（ＭＴＰ）の経路選択の点コードおよびサブシステム番号である。ＬＡＴＡ内経路選択が必要な場合には、サービス・プロバイダーのＳＣＰのアドレスは、ネットワーク間変換のタイプおよびグローバル名称の値である。

上で触れたように、本発明の制約のひとつは、それぞれの加入者電話番号について、それぞれのトリガは１つのサービス・プロバイダーのみを呼び出すことが

できる、ということである。従って、ステップ１５２で示す探索は、この特定の加入者電話番号のこの特定のトリガが、サービス・プロバイダーＳＣＰ４７を通って等１つのサービス・プロバイダーにより、または図１に示すＳＣＰ２６等の市内サービス制御点により市内交換会社を通って等市内交換会社により、のどちらかでサービスされ得る、ということが理解されるべきである。

取り次ぎアクセスＳＣＰ２６’のデータベース４５が受け取られたデータパケットのトリガに対応する情報を含んでいない場合には、ステップ１５３でデータパケットが拒絶され、点１５４でルーチンから抜ける。データベース４５がかかる情報を含んでいる場合には、ステップ１５６で、取り次ぎアクセスＳＣＰ２６’が、データベース４５内のデータパケットに関連する第１のトランザクション番号、発信点コード、およびサブシステム番号を記憶する。好ましくは、第１のトランザクション番号、発信点コード、およびサブシステム番号は、そのデータパケットの第１のトランザクション識別子を含む。この第１のトランザクション識別子は、第１のトランザクション番号、発信点コード、およびサブシステム番号、の連結によって作り出される。この記憶された情報は、ステップ１７０－１７６に関して以下に説明する応答および他のメッセージの取り次ぎに関して取り

次ぎアクセスＳＣＰ２６’によって求められる。

ステップ１５８で、取り次ぎアクセスＳＣＰ２６’は、取り次ぎアクセスＳＣＰ２６’とサービス・プロバイダーのＳＣＰ４７の間のデータ信号経路においてまたは取り次ぎアクセスＳＣＰ２６’とＳＳＰ１５－１５’等のネットワーク要素の間のデータ信号経路において用いられるデータパケットと関連する第２のトランザクション番号を作り出す。この第２のトランザクション番号は、データベース４５内に記憶される第１のトランザクション識別子の代わりに用いられる。本発明において、取り次ぎアクセスＳＣＰ２６’は、現在使わない乱数（または疑似乱数）をデータパケットに割り当てることによって、現在使わない第２のトランザクション番号をデータパケットに割り当てる。取り次ぎアクセスＳＣＰ２６’は、当業者によく知られているように、疑似乱数ジェネレータから乱数を取得する。「現在使われていない」乱数とは、ネットワークを通して、進行中のデータパケットに割り当てた乱数の経過を取り次ぎアクセスＳＣＰ２６’が追っている、ということを意味する。取り次ぎアクセスＳＣＰ２６’は、データパケットに乱数を割り当てる前にそのデータベース４５内のリストまたはテーブルに情報を求め、選択された乱数が進行中のデータパケットの乱数と重複しないということが確認される。

好ましくは、取り次ぎアクセスＳＣＰ２６’は、割り当てられた第２のトランザクション番号を、データベース４５内の上記リストまたはテーブル内に記憶する。乱数をデータパケットの第２のトランザクション番号として用いることにより、第２のトランザクション番号が決して第１のトランザクション番号と相関していないということが確かめられる。このようにして、第２のトランザクション番号は、データパケットの受領者に何ら情報を与えない。乱数を第２のトランザクション番号として用いることにより、メッセージの発信者が、ライバルが用いそうなトランザクション番号を計算してライバルの顧客の発呼を制御しようとすることが防止される。また、このように乱数を用いることによって、メッセージの発信者が自身の発呼に割り当てられたトランザクション番号を分析することによってライバルの発呼に割り当てられたトランザクション番号を推測することも

防止される。

取り次ぎアクセスＳＣＰ２６’が第２のトランザクション番号を作り出した後、ステップ１６０で、取り次ぎアクセスＳＣＰ２６’は、データベース４５内に、第１のトランザクション識別子への第２のトランザクション番号の写像を維持する。好適な実施例で、取り次ぎアクセスＳＣＰ２６’はまた、第２のトランザクション番号を、データパケットの受信宛先点コードと関連するデータベース４５内のテーブルに入力する。データパケットの受信宛先がサービス・プロバイダーのＳＣＰ４７である場合には、受信宛先点コードは、サービス・プロバイダーのＳＣＰ４７の点コードである。さらに、好適な実施例は、データパケットの受信宛先点コードを第２のトランザクション番号と関連づけ、この情報の組み合わせの写像を第１のトランザクション識別子に維持する。さらに、ＳＣＰから発信されるメッセージに関して、取り次ぎアクセスＳＣＰ２６’は、最初のメッセージの被呼者のアドレスのフィールド内の加入者電話番号を、目標ネットワーク要素の受信宛先点コードおよびサブシステム番号に写像せねばならない。これによっ

て、受信宛先加入者が実際にサービス・プロバイダーの顧客であることが保証される。

ステップ１６２で、取り次ぎアクセスＳＣＰ２６’は、データパケットから第１のトランザクション識別子に対応する情報を取り去り、ステップ１６４で、取り次ぎアクセスＳＣＰ２６’は、第２のトランザクション番号をデータパケットに用いる。かかる代用によって、データパケットから何らかの通信トランザクション情報を得ることが、不可能ではないにしても困難になるので、第２のトランザクション番号を第１のトランザクション識別子の代用とすることによって、高度インテリジェントネットワークのインテグリティは維持される。第１のトランザクション識別子を取り去って第２のトランザクション情報を代用した後、ステップ１６６で修正されたパケットはその受信宛先に送られ、点１６８でルーチンから抜ける。

再びステップ１５０を参照して、受け取られたデータパケットが照会ではない

場合には、データパケットは応答（応答メッセージまたは会話型メッセージとも呼ばれる）に相当する。妥当な応答つまり会話型メッセージについては、データパケットは、元々取り次ぎアクセスＳＣＰ２６’が割り当てた第２のトランザクション番号を含むべきである。従って、ステップ１７０で、取り次ぎアクセスＳＣＰ２６’は、トランザクション番号を応答データパケットと関連して比較し、トランザクション番号をデータベース４５内で維持されている活動状態の第２トランザクション番号のリストと比較する。

好適な実施例において、サービス・プロバイダーのＳＣＰ４７から受け取る応答に関して、取り次ぎアクセスＳＣＰ２６’は、別の比較を行う。取り次ぎアクセスＳＣＰ２６’は、応答内のある情報を、応答メッセージに対応する照会を受け取る結果として記憶されたデータベース４５内のある情報と比較する。特に、取り次ぎアクセスＳＣＰ２６’は、応答内の以下の情報－受け取られたトランザクション番号およびサービス・プロバイダーのＳＣＰ４７のＳＳ７の発信アドレス（または点コード）－を、データベース４５内の以下の情報－データパケットの第２のトランザクション番号および照会であったときの受信宛先点コード－と比較する。比較されたトランザクション番号と点コードは、好ましくは、継続される取り次ぎについて合わねばならない(match for)。サービス・プロバイダーのＳＣＰ４７と関連するトランザクション番号間および点コード間の対応を必要とするということを含む、好適な実施例の二重のチェックによって、本発明は、明らかな利点を提供する。この二重チェックシステムは、サービス・プロバイダーの応答の経路が故意でなく直接ＳＳＰへと選択される（例えば、市内交換会社のＳＴＰの経路選択テーブルにおけるエラーのために）ことの悪用から保護し、「不正な」ＳＳ７プロトコルの回線から保護する。

再び図５を参照して、ステップ１７２で、取り次ぎアクセスＳＣＰ２６’は、上に説明したように受け取られたデータパケットと関連する情報がデータベース４５内の情報と対応しているかどうかをチェックする。そうでない場合には、対応していないということは、無効なトランザクション番号を用いた高度インテリジェントネットワーク要素から照会でないメッセージが受け取られた、というこ

とを意味する。この場合には、ステップ１７３でデータパケットは拒絶され、ステップ１７４でルーチンから抜ける。

受け取られた情報が記憶されている情報と対応する場合には、ステップ１７６で、取り次ぎアクセスＳＣＰ２６’はデータベース４５から受け取られた（第２の）トランザクション番号に対応する第１のトランザクション識別子を取得する。第１のトランザクション識別子を呼び出すと、取り次ぎアクセスＳＣＰ２６’は、そのデータパケットのさらなる経路選択または受信宛先の情報を取得する。この受信宛先情報は、点コードおよびサブシステム番号、またはネットワーク間の変換のタイプおよびグローバル名称の値を含んでもよい。取り次ぎアクセスＳＣＰ２６’は、受け取られたデータパケットからそのアドレス情報を取り去り、データベース４５から取得した受信宛先情報を加え、そのデータパケットがＳＳＰその他以前のデータパケットが発信された要素へ戻されるようにする。ルーチンは進んで、ステップ１６６で修正されたパケットを送り、ステップ１６８で抜ける。

１実施例において、本発明はさらなる比較または妥当性検査の手順を行い、応答データパケットがトランザクションを開始したデータパケットと対応するということを決定する。これらのさらなる妥当性検査の手順は、それぞれの応答ＴＣＡＰメッセージのアンパックおよび特定のパラメータの値のそれぞれの検査を含み、パラメータの値が最初のデータパケット内の対応する特定のパラメータの値と対応するということを決定する。最初のデータパケット内には存在していなかったり、あるいはその値がサービス・プロバイダーによって変えられたパラメータについてのみ、取り次ぎ手順が必要である。従って、応答データパケットのパラメータの値における、最初のデータパケット内のパラメータの値からの変化の検査を行うために、取り次ぎアクセスＳＣＰ２６’は、最初のデータパケットのパラメータの値の記録を、データベース４５内に維持している。

図６は、ある特定のタイプの高度インテリジェントネットワークのメッセージについて好適な実施例が実行する取り次ぎのプロセスを示す。図示の各手順は取り次ぎアクセスＳＣＰ２６’が実行する、ということが理解されるべきである。

承認されたアクティビティに関する照会は、データベース４５（図２）内の様々なテーブル内に記憶されている。この部分の取り次ぎ処理がステップ１８０で入力され、ここで取り次ぎアクセスＳＣＰ２６’がデータパケットを受け取る。ステップ１８２で、取り次ぎアクセスＳＣＰ２６’が、データパケット内の特定の中継回線のグループの経路選択の何らかの要求があるかどうかをチェックする。何ら中継回線のグループが要求されない場合には、妥当な中継回線のグループの要求１８６の周囲にループを描くＮＯの枝路１２６を通ってステップ１８８へと進む。１個またはそれ以上の中継回線のグループが要求される場合には、ステップ１８６で、取り次ぎアクセスＳＣＰ２６’が、そのデータパケットを生成したサービス・プロバイダーの、およびそのデータパケットが向かうＳＳＰの、法定の中継回線のグループのルートインデックスのテーブルをチェックする。

妥当な中継回線のグループのこのテストは、要求内で指定されたそれぞれの中継回線のグループについて行われる、というのも、その代わりに用いることのできる多数の中継回線のグループを中継回線のグループの経路選択の要求において指定してもよいからである。要求された中継回線のグループのうちのいずれか１個でもこのサービス・プロバイダーのＳＣＰによる使用が承認されていない場合には、ステップ１８６からＮＯの枝路へと進み、これは、ステップ１８７Ａにおけるデータパケットの拒絶、ステップ１８７Ｂ（オプション）におけるデフォルト・アプリケーションの供給、およびステップ１８７Ｃにおけるルーチンからの

抜け、に通じる。サービス・プロバイダーのＳＣＰが中継回線のグループの経路選択の要求に含まれるそれぞれの中継回線のグループを用いることが承認されている場合には、処理は次の手順であるステップ１８８へと進む。

好適な実施例は、承認されていない中継回線のグループを用いる可能性のある何らかの要求が検出される場合にはメッセージを拒絶する、ということに注目するべきである。取り次ぎアクセスＳＣＰにデータパケットを再構成させて、承認されていない中継回線のグループは削除するがサービス・プロバイダーのＳＣＰが用いることを承認されている１個またはそれ以上の中継回線のグループは含むようにすることも可能である。しかし、中継回線のグループの経路選択の適切な

要求をするという責務は、サービス・プロバイダーに負わせることが好ましいと考えられる。

ステップ１８８で、データパケットがテストされ、交換機でない高度インテリジェントネットワーク要素へのアクセスが要求されているかどうかが確かめられる。上で触れたとおり、ある特定の加入者電話番号への発呼に影響を与えることへの承認は、その加入者電話番号を取り扱う交換機と関連するＳＳＰと通信することへの承認を暗示している。しかし、他のサービス制御点またはサービス接続点等の交換機でない高度インテリジェントネットワーク要素へのアクセスを求めるデータパケットについての別個のテストが含まれている。

これまでのテストと同様、交換機でない高度インテリジェントネットワーク要素が要求されている場合には、ステップ１８８から承認のテスト１９０の周囲にループを描くＮＯの枝路を通ってステップ１９２へと進む。メッセージの要求が交換機でない高度インテリジェントネットワーク要素へのアクセスの要求を含む場合には、ＹＥＳの枝路を通ってステップ１９０へと進み、ここで加入者電話番号のテーブルが情報を求められてその交換機でない高度インテリジェントネットワーク要素の加入者電話番号がこの特定のサービス・プロバイダーのＳＣＰの承認された加入者電話番号のリストに含まれているかどうかが決定される。従来は交換機ではない高度インテリジェントネットワーク要素に割り当てられてきた交換機でない要素の指定を、その加入者電話番号で記憶するのが好ましい、ということに注目するべきである。加入者電話番号は、交換機でない要素を指定する好適な方法である。これにより、サービス・プロバイダーがＳＳ７の点コードを知ったり用いる必要がなくなることにより、ネットワークのセキュリティがさらに与えられる。この場合、加入者電話番号は、ステップ１５２（図５）に関して上に説明した加入者電話番号の妥当性検査と同様に、ある特定の加入者回線または加入者専用中継回線に関連する加入者電話番号なのではない、ということに注目するべきである。

再びステップ１９０を参照して、サービス・プロバイダーのＳＣＰが要求されている交換機でない高度インテリジェントネットワーク要素にアクセスすること

を承認されていない場合には、ＮＯの枝路へと進み、これは、ステップ１８７Ａにおけるデータパケットの拒絶、ステップ１８７Ｂ（オプション）におけるデフォルト・アプリケーションの供給、およびステップ１８７Ｃにおけるルーチンからの抜け、に通じる。サービス・プロバイダーのＳＣＰが承認されている場合には、ＹＥＳの枝路からステップ１９２へと進む。ステップ１９２で、チェックが行われ、データパケットが限られた資源の使用を求めているかどうかを決定する。好適な実施例は、限られた資源というものを、ある限られた数存在し、いかなる与えられたサービス・プロバイダーによって占有される時間をも厳密に制御する必要がある、少なくとも１個のクラスのネットワーク資源である、と定義する。本明細書において用いる概念では次のようには限定しないが、限られた資源というのは、通常、リアルタイムの発呼への音声接続に関係し発呼者から供給されるかまたは発呼者に送られるかのどちらかの音声信号のある形式を処理する装置である。かかる装置に共通の特性は、使用されるとき毎に比較的長時間用いられる、ということである。好適な実施例においては、交換ディジット受信機および音声による告知の装置が、限られた資源として分類される。しかし、本発明の他の実施例では、他の装置を限られた資源として分類してもよく、実際、本発明の実施について定義される多数の階層的クラスの資源があり得る。

限られた資源が何ら要求されない場合には、取り次ぎのテストのパスに成功し、ＮＯの枝路へと進み、ステップ１８４でルーチンから抜ける。限られた資源が要求されている場合には、ＹＥＳの枝路からステップ１９４へと進む。この手順は、サービス・プロバイダーのＳＣＰがこの資源またはこの資源のクラスを用いるこ

とを承認されているかどうかをテストするものである。このテストに添わなければ、ＮＯの枝路に進みステップ１８４でルーチンから抜ける。再びステップ１９４を参照して、サービス・プロバイダーのＳＣＰが資源を用いることを承認されている場合には、ＹＥＳの枝路からステップ１９６へと進み、ステップ１９６で好適な実施例の重要な取り次ぎ機能がテストされる。好適な実施例が限られた資源として定義するネットワーク資源のクラスは通常用いられる毎に長時間占有さ

れる装置を含むので、好適な実施例の方法は、与えられたサービス・プロバイダーが同時に占有することのできるかかる装置の数に制限を設けている。この上限を資源占有数と呼び、これは単に、サービス・プロバイダーまたはそのアプリケーションが同時に占有してもよい限られた資源の装置の所定の数である。

資源占有数は、収容できるサービス・プロバイダーの数からの最大許容数によってのみ選択するのではなく、料金に応じて決めるのが好ましいと思われる。従って、音声による告知装置を大量に用いると予想するサービス・プロバイダーは、それらの資源へのアクセスを設けることについて市内交換会社により高い料金を払って、比較的多数のそれらの資源を同時に占有することができるようにする必要がある。

限られた資源または資源のクラスの総数の代わりに、またはそれに加えて用いてもよい、資源占有数を定義する他の方法もある。特に、ひとつのサービスが占有する限られた資源の総数のみでなく、与えられた資源の所有者における、すなわち与えられた交換機または与えられたサービス接続点における限られた資源の総数も制限する、ということが重要である。例えば、あるサービス・プロバイダーのＳＣＰがアクセスしてもよいある特定のサービス接続点に５本の音声による告知の回線がある場合、ひとつのサービス・プロバイダーのＳＣＰが同時に５本全部の回線を占有してネットワーク上で実行されている他のアプリケーションに音声回線を提供することを妨げることはできない、ということを確かめることが重要である。これは、本発明の実施例における資源占有数に特有の定義となりうる。さらに、サービスのアプリケーションが、ネットワーク内の様々な資源の所有者の中でその数の限られた資源よりも多くを占有することが許されている場合であっても、これをさらなる制限として指定してもよい。

本発明の方法は、好ましくは、ひとつのサービス・プロバイダーのアプリケーションが同時に占有してもよい限られた資源の数の所定の上限である資源占有数を規定する。このシステムは、それぞれのサービス・プロバイダーのアプリケーションについての数が増える方向／減る方向へのカウントとして、限られた資源のカウントを維持する。ステップ１９６に達すると、取り次ぎアクセスＳＣＰ２

６’は、このサービス・プロバイダーについての限られた資源のカウントが現在資源占有数を超えているかどうかをテストする。このテストが真である場合、ＹＥＳの枝路へと進み、これは、ステップ１８７Ａにおけるデータパケットの拒絶、ステップ１８７Ｂ（オプション）におけるデフォルト・アプリケーションの供給、およびステップ１８７Ｃにおけるルーチンからの抜け、に通じる。限られた資源の使用を要求する顧客にサービスを提供するために、リトライの試み等の問題に取り組むことは、サービス・プロバイダーの義務である。

限られた資源のカウントがまだ資源占有数よりも小さい場合には、ステップ１９６からＮＯの枝路をとってステップ１９８へと進み、ここで限られた資源のカウントがインクリメントされる。ステップ１９８の後、処理は進んで、ステップ１９９でルーチンから抜ける。

図示していない会話の終了を取り扱う他のルーチンには、その特定のサービス・プロバイダーが要求する限られた資源のユーザが完了したときにはいつでも限られた資源のカウントをディクレメントする責任がある、ということに注目するべきである。数が増える方向／減る方向へのカウントの体系の実施は、当業者には簡単でありよく知られている。

１実施例において、本発明は、少なくともう１つの妥当性検査または取り次ぎ手順を行う。特に、取り次ぎアクセスＳＣＰ２６’は、料金番号および交互のビリング番号に対応する応答データパケット内のパラメータの値に関して気付かれる変化を検査する。料金番号にまたは交互のビリング番号に対応する応答データパケット内のパラメータの値が最初のデータパケット内の値から変化する場合には、取り次ぎアクセスＳＣＰ２６’が、変化した値（料金番号、交互のビリング番号、あるいはその両方）を、サービス・プロバイダーの顧客の加入者電話番号のリストに関するデータベース４５内の情報と比較する。変化した値と加入者

電話番号のリストの間に符合が見つからない場合には、取り次ぎアクセスＳＣＰ２６’は、応答データパケットを拒絶する。

本発明はまた、取り次ぎアクセスＳＣＰ２６’がサービスするサービス・プロバイダーのＳＣＰの状態の監視において取り次ぎアクセスＳＣＰ２６’が達成す

る各手順によってネットワークを管理する方法を提供する。この管理方法の１態様は、取り次ぎアクセスＳＣＰ２６’が、サービス・プロバイダーのＳＣＰが応答メッセージを戻すのにかかる時間の経過を追う、というものである。サービス・プロバイダーのＳＣＰが応答メッセージを戻すのに、指定した最小時間よりも長く時間がかかる場合には、取り次ぎアクセスＳＣＰは、メッセージのいくつかを廃棄することによって、サービス・プロバイダーの新しいメッセージの負荷を減らす手段を講じる。サービス・プロバイダーが、廃棄されるメッセージのデフォルト・アプリケーションを指定している場合には、取り次ぎアクセスＳＣＰは、好ましくは、かかるデフォルト・アプリケーションをそれぞれの廃棄されるメッセージに供給する。取り次ぎアクセスＳＣＰがデフォルト・アプリケーションを供給しない場合には、交換機は、例えば電話サービス（ＰＯＴＳ）等の標準のデフォルト処理をしてメッセージを供給する。

図７は、取り次ぎアクセスＳＣＰ２６’にサービスされるサービス・プロバイダーのＳＣＰ４７の状態を監視する管理方法を示すフローチャートである。ステップ２００で、取り次ぎアクセスＳＣＰ２６’は、データパケットの経路をサービス・プロバイダーのＳＣＰ４７へと選択し、ステップ２０２で、取り次ぎアクセスＳＣＰ２６’は、サービス・プロバイダーのＳＣＰ４７が応答メッセージを戻すのにかかる時間の量に関するタイマをスタートさせる。決定のステップ２０４で、取り次ぎアクセスＳＣＰ２６’は、タイマが切れたかどうかをチェックする。このタイマーの値は、好ましくは、スイッチタイマ(switch timer)よりも約２秒小さい値に設定されている。タイマが切れていない場合には、ＮＯの枝路をとって、タイマが切れるまでタイマが切れたかどうかをチェックする手順を繰り返す。いったんタイマが切れると、ステップ２０６で、取り次ぎアクセスＳＣＰ２６’が、応答が受け取られたどうかをチェックする。そうである場合には、ステップ２０８でルーチンから抜ける。応答が受け取られていない場合には、ステ

ップ２１０で、取り次ぎアクセスＳＣＰ２６’が、サービス・プロバイダーがデフォルト処理またはアプリケーションが供給されるよう指定したかどうかをチェックする。そうである場合には、ステップ２１２で、取り次ぎアクセスＳＣＰ２

６’が、指定されたデフォルト処理を供給する。サービス・プロバイダーがデフォルト処理を供給していない場合には、ステップ２１２のデフォルト処理の供給の周囲にループを描くステップ２１０のＮＯの枝路をとって、ステップ２１６へ進む。ステップ２１６で、取り次ぎアクセスＳＣＰ２６’は、サービス・プロバイダーのＳＣＰのメッセージの負荷を減らすべきかどうかをチェックする。サービス・プロバイダーのＳＣＰのメッセージの負荷を減らす決定は、上に説明したタイマ機能によって供給される情報をベースにした予め選択した時間の期間内に１つまたはそれ以上の応答メッセージを戻せないということを含む、様々な要因をベースにしてもよい。メッセージの負荷が減らされるべきでない場合には、ルーチンは進んでステップ２０８で抜ける。メッセージの負荷が減らされるべき場合には、ステップ２１８で、取り次ぎアクセスＳＣＰ２６’は、サービス・プロバイダーのＳＣＰ４７に向けられた次の新しい照会を廃棄することによってメッセージの負荷を減らすことに進む。前と同様、サービス・プロバイダーがデフォルト処理を指定している場合には、ステップ２２０で、取り次ぎアクセスＳＣＰ２６’が、廃棄された新しい照会にかかるデフォルト処理を供給する。指定したデフォルト処理の供給の後、ルーチンはループを描いて決定のステップ２１６に戻り、サービス・プロバイダーのＳＣＰのメッセージの負荷が減らされるべきかどうかをチェックする。サービス・プロバイダーのＳＣＰのメッセージの負荷を減らす交互のまたはさらなる手段は、負荷のかかりすぎたサービス・プロバイダーの顧客に役立っているＳＳＰ１５－１５’等のＳＳＰに、取り次ぎアクセスＳＣＰ２６’によって自動発呼ギャッピング（ＡＣＧ：Automatic Call Gapping）のメッセージを供給することである。好ましくは、取り次ぎアクセスＳＣＰは、メッセージの流量を監視し、特に、取り次ぎアクセスＳＣＰがサービスするサービス・プロバイダーが用いるそれぞれの終端トリガ・メッセージの流量を監視する。取り次がれたＳＣＰが、サービス・プロバイダーのＳＣＰが負荷がかかりすぎになっているということを検出する場合には、取り次ぎアクセスＳＣＰは、負

荷のかかりすぎたサービス・プロバイダーの顧客に役立っているＳＳＰに、自動発呼ギャッピングのメッセージを送る。負荷を減らしてもタイミングの問題が解

決されない場合には、取り次ぎアクセスＳＣＰは、サービス・プロバイダーのＳＣＰがアウトオブサービスであると決定する。サービス・プロバイダーのメッセージの負荷が減らされるべきではないと決定されるまでステップ２１６～２２０が繰り返され、ステップ２０８でルーチンから抜ける。

本発明の管理方法の他の１態様は、取り次ぎアクセスＳＣＰが、以前にアウトオブサービスであると決定されたサービス・プロバイダーのＳＣＰの状態を監視する、ということである。好ましくは、取り次ぎアクセスＳＣＰ２６’は、定期的に（１分間に１回等）アウトオブサービスのサービス・プロバイダーのＳＣＰにテストメッセージを送る。１つのテストメッセージ、または一連のテストメッセージがサービス・プロバイダーのＳＣＰに正しく取り扱われる場合には、サービス・プロバイダーのＳＣＰへの呼量は、取り次ぎアクセスＳＣＰ２６’によって自動的に再開される。

さらに、本発明はまた、メッセージの失敗に関するセキュリティの監査証跡の維持にも備える。取り次ぎの失敗および高度インテリジェントネットワークのメッセージの失敗（プロトコルのエラー、拒絶、戻りのエラー、アプリケーションのエラー、等）はすべて、監査できる事象であると考えられる。監査できる事象には、トランザクションを確立しようとする無効な試み、データにアクセスしようとする無効な試みについてのすべての記録、およびセキュリティ処理の構成のすべての変化、を含む。それぞれの監査できる事象について、監査証跡は、日付、時間、含まれるＴＣＡＰメッセージ（ＭＴＰおよびＳＣＣＰのデータを含む）の写し、トリガのタイプおよびトリガする受信宛先番号、および何らかのエラーコード、を含む。本発明において、監査証跡の概念は、高度インテリジェントネットワーク維持パラメータの概念と類似するものとして考えられている。１実施例において、本発明は、受け取るネットワーク要素に、付属のデータパケットのセキュリティの監査を作動させるように要求する、データパケット内のパラメータを含む。セキュリティ・パラメータは、単一の識別子の役割をし、異なるネットワーク要素からの監査の記録をリンクすることによって、監査されるユーザがと

る行動の、ネットワークの広い視野を得ることができるようになっている。セキュリティ・パラメータは、アクセスの失敗を繰り返した後トランザクションが確立したり、通常昼間にのみ操作するユーザが夜間にトランザクションを確立する、等の、普通でないセキュリティの事象が起こるときに作動してもよい。

本発明の管理方法の他の１態様は、取り次ぎアクセスＳＣＰが、サービス・プロバイダーのＳＣＰの選択された加入しきい値に従って、およびネットワークの容量に従って取り次ぎアクセスＳＣＰが役立つサービス・プロバイダーのＳＣＰに入ってくる方とそこから出ていく方の両方のメッセージの流量を監視し管理する、というものである。特に、サービス・プロバイダーのＳＣＰ４７は、メッセージの流量に関して加入しきい値を与えられている。取り次ぎアクセスＳＣＰ２６’は、サービス・プロバイダーのＳＣＰへのメッセージの流れが、少なくともネットワークのメッセージの呼量をベースにした加入しきい値に達するのを許す。サービス・プロバイダーのＳＣＰ４７へのメッセージの流量が加入しきい値を超える場合には、メッセージの経路をサービス・プロバイダーのＳＣＰ４７へと選択することを継続するかどうかを決定するために、取り次がれたＳＣＰ２６’がネットワークのメッセージの呼量を評価する。取り次ぎアクセスＳＣＰ２６’がその容量を有する場合には、好適な実施例において、取り次ぎアクセスＳＣＰ２６’は、メッセージの流量の加入しきい値を超えていても、メッセージの経路をサービス・プロバイダーのＳＣＰ４７へと選択することを継続する。取り次ぎアクセスＳＣＰ２６’に負荷がかかりすぎている場合には、サービス・プロバイダーＳＣＰ４７への照会を拒絶する（応答メッセージとは対照的に）。拒絶されたメッセージのデフォルト・アプリケーションをサービス・プロバイダーのＳＣＰ４７が選択している場合には、取り次ぎアクセスＳＣＰ２６’がデフォルト・アプリケーションを用いる。

取り次ぎアクセスＳＣＰ２６’のメッセージの負荷を減らす交互のまたはさらなる手段は、ＳＳＰ１５－１５’等のＳＳＰに、取り次ぎアクセスＳＣＰ２６’によって自動発呼ギャッピング（ＡＣＧ）のメッセージを供給することである。好ましくは、以下に図８に関して説明するように、取り次ぎアクセスＳＣＰ２６’は、メッセージの流量を監視し、特に、取り次ぎアクセスＳＣＰ２６’がサー

ビスするサービス・プロバイダーが用いるそれぞれの終端トリガ・メッセージの流量を監視する。取り次ぎアクセスＳＣＰ２６’が負荷がかかりすぎになっているということを検出する場合には、取り次ぎアクセスＳＣＰ２６’は、取り次ぎアクセスＳＣＰ２６’が役立っているサービス・プロバイダーの顧客に役立っているＳＳＰに、自動発呼ギャッピング（ＡＣＧ）のメッセージを送る。

図８は、本発明の流量の監視および管理を示すフローチャートである。ステップ２４０でデータパケットを受け取ると、ステップ２４２で、取り次ぎアクセスＳＣＰ２６’が、送信者の識別子のデータパケットの適切なフィールドをチェックする。送信者の識別子は、そのメッセージを作り出したエンティティを識別するコードである。ルーチン２４４において、ステップ２４２で識別された送信者と関連する現在のカウントがインクリメントされ、適切なタイマの値が記憶される。これらのカウントは、いくつかの目的のために維持される。そのひとつは、第三者のサービス・ブロバイダーに高度インテリジェントネットワークの使用について課金するためにある特定の送信者が生成する照会／応答のペアのカウントを維持する、ということである。さらに、サービス・プロバイダーの動作しているＳＣＰ４７からインターフェース４８を横切ってパケットメッセージが供給される入メッセージの流量が計算される。この入メッセージの流量は、比較的短期間にわたる平均である。さらに、過度のメッセージ呼量の警告状態が検出できるように、より長期間の平均が維持される。好適な実施例においては、所定の値を超える短期間の入メッセージの流量のみによって、インターフェース４８がブロックされる。

ステップ２４６で、計算した入メッセージの流量が、その特定のサービス・プロバイダーの承認されたメッセージの流量数と比較される。この数は、取り次ぎアクセスＳＣＰ２６’内のデータベース４５内のサービス・プロバイダーの記録内に記憶されている。確立された判定基準によって入メッセージの流量が過剰である場合には、ＹＥＳの枝路からルーチン２４８へと進み、ここで、取り次ぎアクセスＳＣＰ２６’によって、サービス・プロバイダーのＳＣＰ４７に通知するメッセージが、インターフェース４８を横切って送信し戻される。これによって、サービス・プロバイダーのＳＣＰは、示したものよりも大きいインターフェー

ス

４８を横切るメッセージを送信する流量が用いられる場合には、とることのできる何らかの適切な行動をとることができる。

ここから、ルーチンは決定のステップ２５０へと進み、ここで入メッセージの流量が承認されたメッセージの流量を超えている程度がチェックされる。入メッセージの流量が、少なくともネットワークが他のサービス・プロバイダーに適切にタイムリーにサービスを提供することのできる能力が損なわれる等の所定の量だけ、承認されたメッセージの流量数を超えている場合には、取り次ぎ処理は、物理的なポートおよびブロックのインターフェース４８を横切るメッセージの動きを終了する。このオプションが要求される場合には、ステップ２５０からＹＥＳの枝路へと進む。反対に、入メッセージの流量は大きすぎるがネットワークの性能をひどく低下させるほど過剰ではない場合には、ステップ２５０からＮＯの枝路へと進む。

最初に、入メッセージの流量が、少なくとも上述の所定の量だけ承認されたメッセージの流量数を超えている状況を考える。論理はステップ２５２へと進み、ここで、ＳＴＰ２０’に終了のメッセージが送られる。これは、ＳＴＰに、インターフェース４８を横切る入呼量を終了するように、従ってそれによって表される物理的なポートをブロックするように、命令する。次に、ステップ２５４に達し、ここでＳＣＰは、サービス管理システム（図１）に、ＳＳ７データリンク４６のポート４８におけるアクセスの終了を通知する。これによって、サービス管理システムにおける人員は、そのアクセスが遮断されているサービス・プロバイダーにコンタクトをとって、是正処置をとることができるかどうか調べる機会が与えられる。さらに、これによって、この特定のサービス・プロバイダーの顧客から苦情があるかもしれないということを見越して、サービス管理システムに終了が通知される。

ステップ２５６で表されるルーチンは、上で説明したデフォルト・アプリケーションの起動である。図２の実施例における、パケットメッセージを行ったり来たりして通すパターンの前の説明より、デフォルト・アプリケーションの一部は

電話局（ＳＳＰ）１５－１５’の１つ内で発信されるパケットに応答してＳＣＰ２６’からＳＳ７データリンク４６にパケットを送る処理を終了することである、

ということが理解される。従って、取り次ぎアクセスＳＣＰ２６’は、通常の取り次ぎ機能を行ってその後パケットをサービス・プロバイダーのＳＣＰ４７へと送るのではなく、通常はサービス・プロバイダーのＳＣＰ４７に送られる受け取られたパケットにどんな応答をデフォルト・アプリケーションが与えるかに関して、決定を行わねばならない。従って、いったんこの状態に入ると、最終的にサービス・プロバイダーのＳＣＰ４７向けに意図されたパケットに応答して取り次ぎアクセスＳＣＰ２６’が外へ送信するその特定のパケットはＳＣＰ２６’上で実行されているデフォルト・アプリケーションに従って修正され、インターフェース４８のブロッキングがクリアされるまでこの状態が優勢である(prevail)、ということが理解されるべきである。従って、ステップ２４６で用いられるテストの一部は、インターフェース４８が既にブロックされているかどうかを決定することである、ということが理解されるべきである。そのような場合には、終了命令を出し続けることは無駄である。

いったんデフォルト・アプリケーションが起動すると、次のパケットが受け取られるまで、ステップ２５８でルーチンから抜ける。

次に、ステップ２５０からＮＯの枝路へと進む状況を考える。まず、決定のステップ２６０が実行され、ここでメッセージを拒絶する判定基準が調べられる。判定基準には、入メッセージの流量が承認されたメッセージの流量数を超える程度、およびメッセージ自体の性質、が含まれる。後者を考えた場合に関し、メッセージは、単に拒絶されその向けられた受信宛先に送られない場合には、顧客の電話をサービスを供給することができない状態にロックしたままにする可能性のあるものであるかもしれない。ステップ２６０の決定がベースにすることができる他の判断基準もある。メッセージが拒絶されないと仮定すると、ＮＯの枝路へと進み、ステップ２４８でルーチンから抜ける。

メッセージが拒絶される場合には、ステップ２６０からＹＥＳの枝路をとり、

ステップ２６２へと進む。この手順で、拒絶メッセージが送信者、今考えている例ではサービス・プロバイダーのＳＣＰ４７、に送信される。メッセージの拒絶は、他のネットワーク要素、特に電話局の交換機におけるＳＳＰ、の動作に悪影響を及ぼす可能性があるので、ステップ２６４で、サービス・プロバイダーから

メッセージを拒絶した結果としてエラーメッセージを生成するべきかどうかに関して決定がなされる。これが適切であるとみなされる場合には、ＹＥＳの枝路からステップ２６６へと進み、ここで、ＳＣＰ４７が応答しようとしていた元々のメッセージを送ったＳＳＰにエラーメッセージが送られる。ここから、ステップ２６８でルーチンから抜ける。エラーメッセージが必要でない場合には当然、ステップ２６４からＮＯの枝路へと進み、ステップ２６８で直接ルーチンから抜ける。

ステップ２４８と２６８の間の各手順の説明は、この方法の論理がステップ２４６で過剰な入メッセージの流量を検出したという過程をベースにした。入メッセージが過剰でない場合には、ステップ２４６からＮＯの枝路へと進み、ステップ２７０で直接ルーチンから抜ける。

前述のことから、本明細書で説明した方法によって、サービス・プロバイダーのＳＣＰと取り次ぎアクセスＳＣＰの間の取り次がれたインターフェースを横切る効果的な取り次ぎが行われる、ということが理解されよう。第１および第２のトランザクション番号を用いることにより、市内交換会社によるネットワークの動作に関する機密に関わる情報へのアクセスやサービス・プロバイダーのライバルに関する情報にアクセスする可能性からサービス・プロバイダーを効果的に分離する。図示の取り次ぎの各手順により、サービス・プロバイダーが生成するメッセージのインテグリティが保証される。さらに、図示の取り次ぎの各手順により、サービス・プロバイダーに与えられ市内交換会社にかかる特権のサポートのために費用を費やさせる高度インテリジェントネットワーク内のある特権の料金を市内交換会社が定めることが強制される。この強制により、いかなる特定のサービス・プロバイダーが、他のサービス・プロバイダーの顧客の不利益になったり市内交換会社の不利益になるようにそのネットワーク内でのあるタイプの資源

の割合が極端に固定することも、防止される。

好適な実施例の前述の説明より、当業者には本発明の他の実施例も示唆され、従って、本発明の範囲は以下の請求の範囲およびその均等物によってのみ限定されねばならない。

【図１】

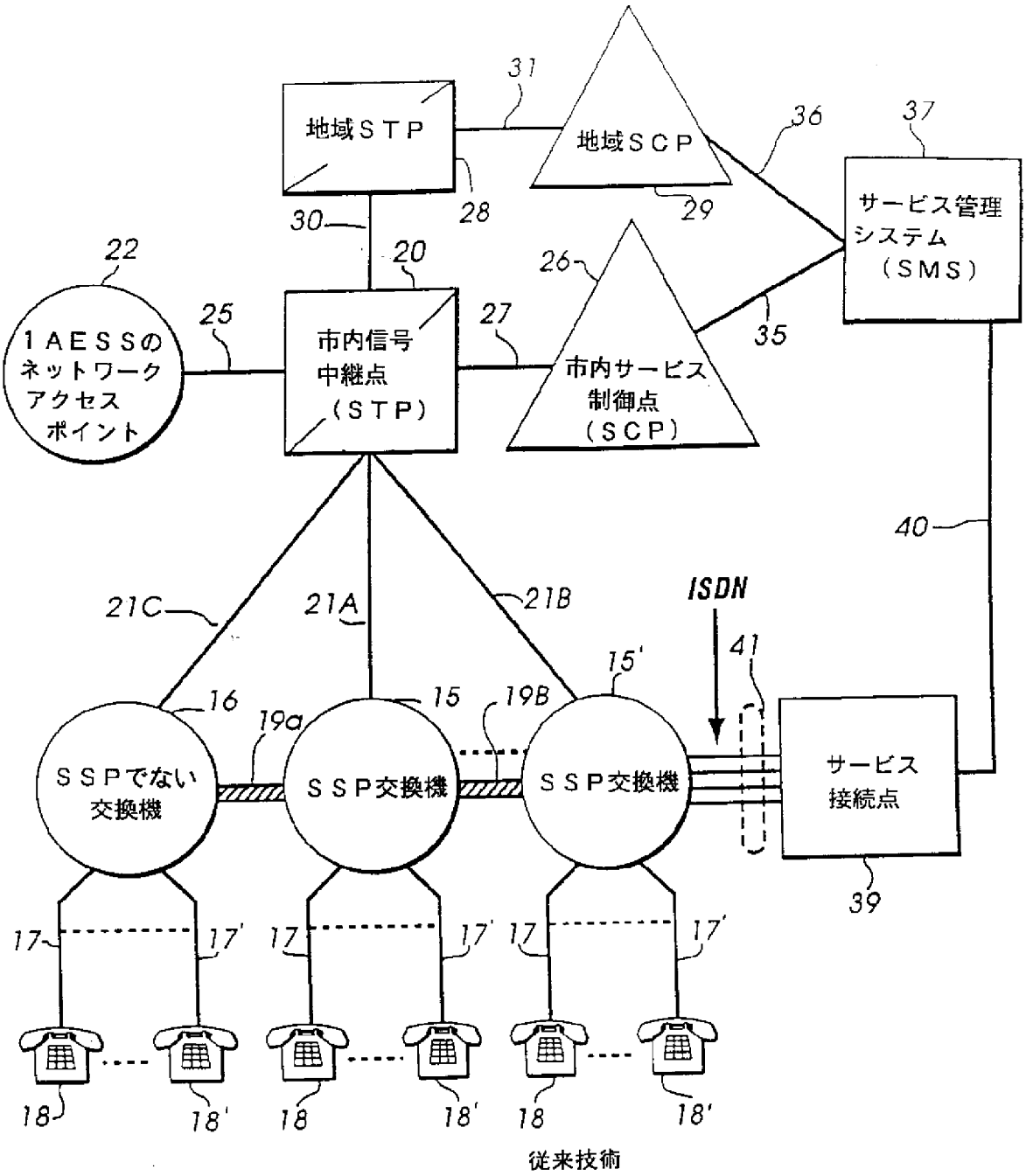
地域ＳＴＰ
地域ＳＣＰ
サービス管理システム（ＳＭＳ）
１ＡＥＳＳのネットワークアクセスポイント
市内信号中継点（ＳＴＰ）
市内サービス制御点（ＳＣＰ）
ＳＳＰでない交換機
ＳＳＰ交換機
ＳＳＰ交換機
サービス接続点
ISDN
22
25
20
26
27
30
31
28
29
36
37
35
40
21C
21A
21B
16
19a
15
19B
15'
41
39
17
17'
18
18'
従来技術

FIG 1

【図２】

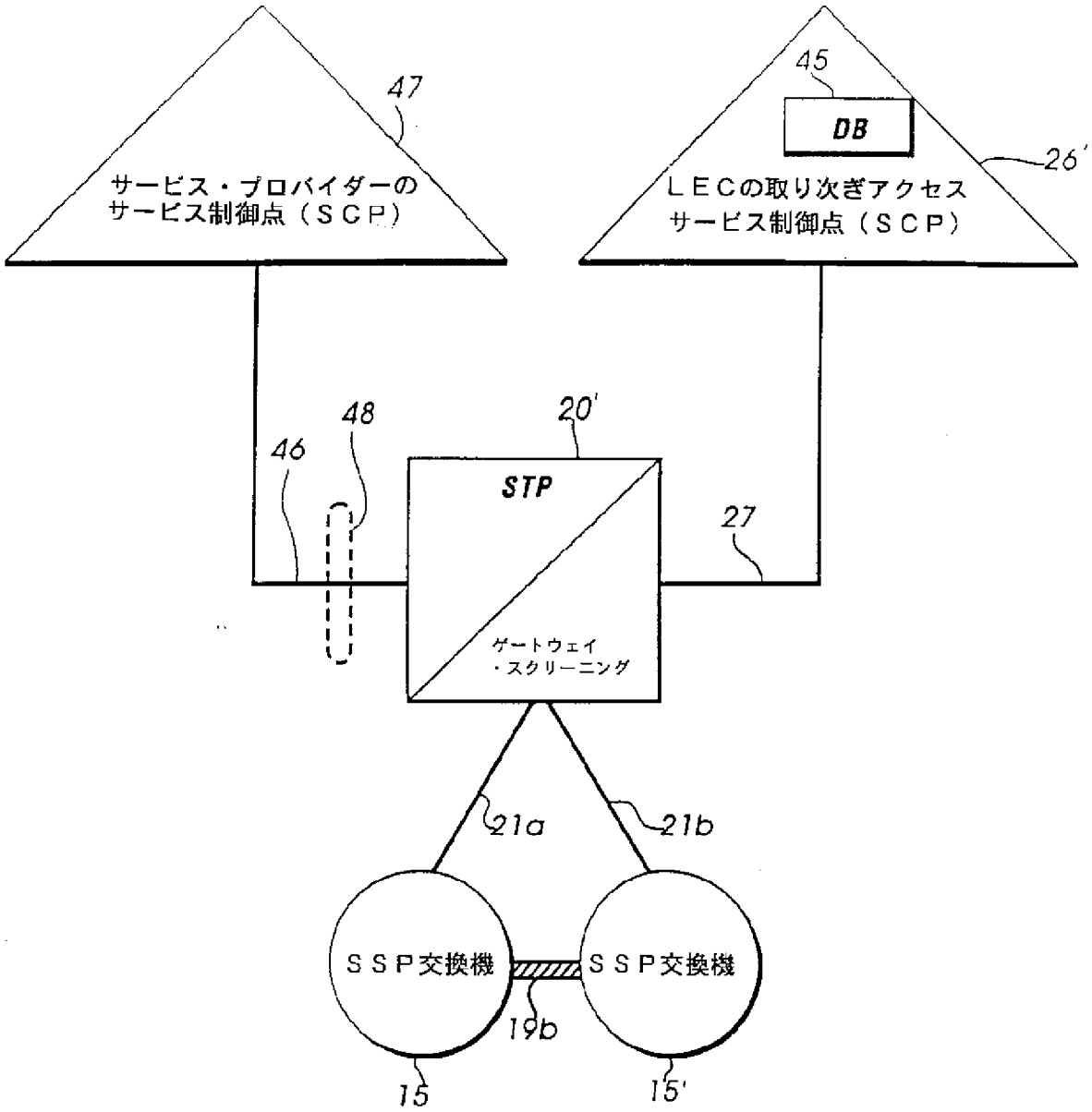
47
サービス・プロバイダーの
サービス制御点（ＳＣＰ）
45
DB
26'
ＬＥＣの取り次ぎアクセス
サービス制御点（ＳＣＰ）
48
20'
46
STP
27
ゲートウェイ
・スクリーニング
21a
21b
ＳＳＰ交換機
ＳＳＰ交換機
19b
15
15'

FIG 2

【図３】

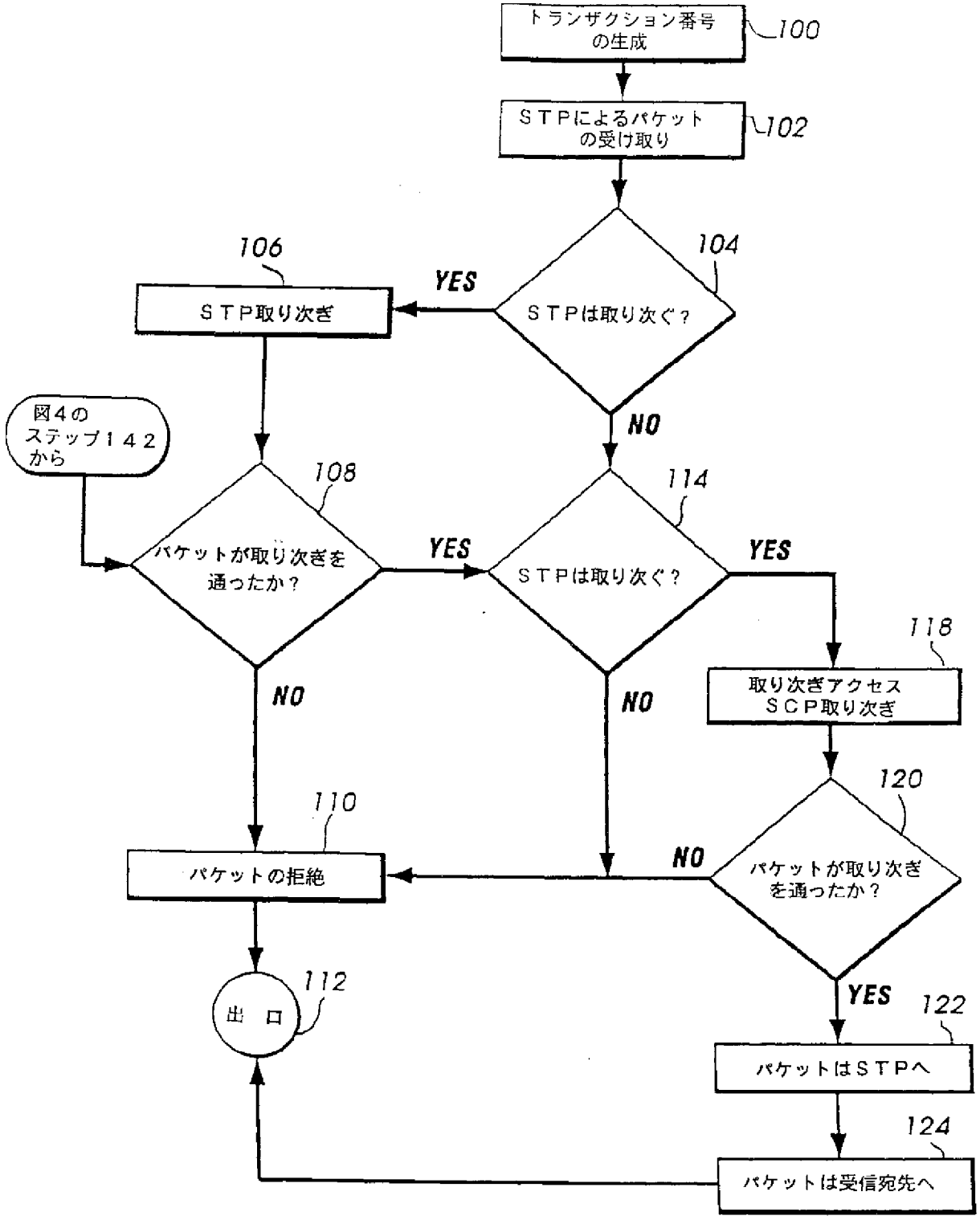
トランザクション番号の生成
100
ＳＴＰによるパケットの受け取り
102
ＳＴＰは取り次ぐ？
104
YES
ＳＴＰ取り次ぎ
106
NO
図４のステップ１４２から
パケットが取り次ぎを通ったか？
108
YES
ＳＴＰは取り次ぐ？
114
YES
NO
NO
取り次ぎアクセスＳＣＰ取り次ぎ
118
パケットの拒絶
110
NO
パケットが取り次ぎを通ったか？
120
出口
112
YES
パケットはＳＴＰへ
122
パケットは受信宛先へ
124

FIG 3

【図４】

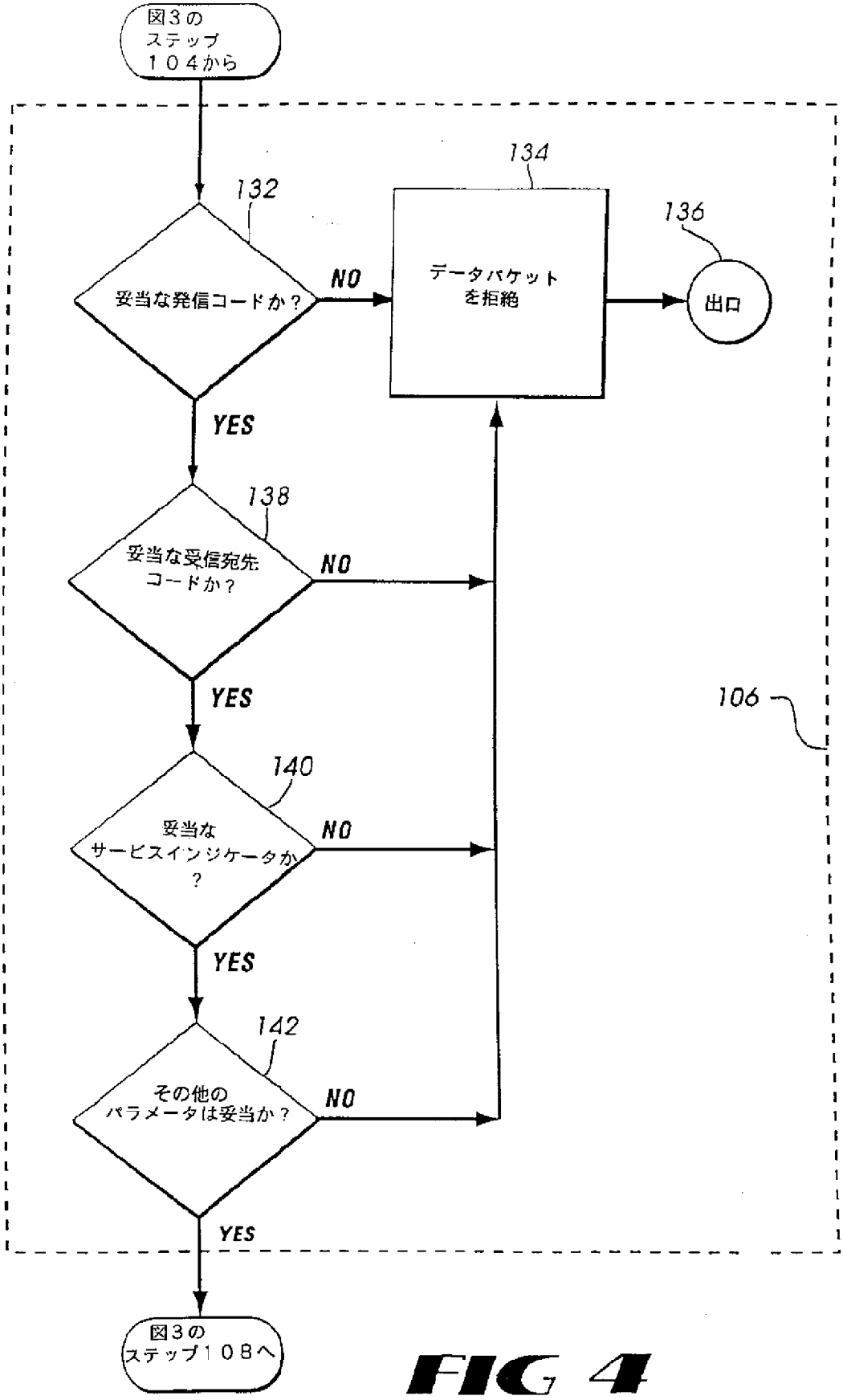
図３の
ステップ
１０４から
132
妥当な発信コードか？
NO
134
データパケット
を拒絶
136
出口
YES
138
妥当な受信宛先
コードか？
NO
YES
106
140
妥当な
サービスインジケータか
？
NO
YES
142
その他の
パラメータは妥当か？
NO
YES
図３の
ステップ１０８へ

FIG 4

【図５】

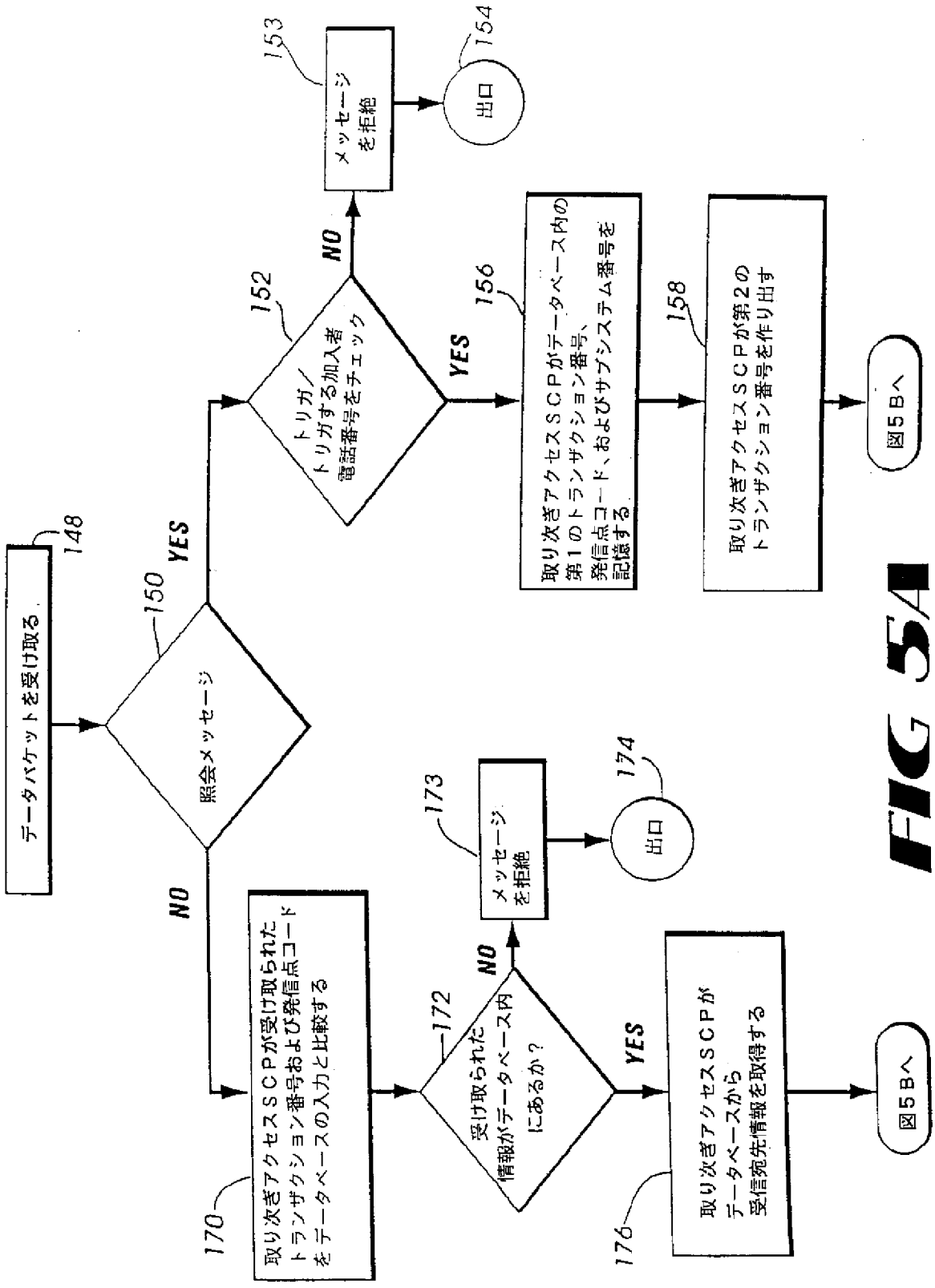
データパケットを受け取る
148
照会メッセージ
150
YES
NO
トリガ／トリガする加入者電話番号をチェック
152
YES
NO
メッセージを拒絶
153
出口
154
取り次ぎアクセスＳＣＰがデータベース内の第１のトランザクション番号、発信点コード、およびサブシステム番号を記憶する
156
取り次ぎアクセスＳＣＰが第２のトランザクション番号を作り出す
158
図５Ｂへ
取り次ぎアクセスＳＣＰが受け取られたトランザクション番号および発信点コードをデータベースの入力と比較する
170
受け取られた情報がデータベース内にあるか？
172
NO
YES
メッセージを拒絶
173
出口
174
取り次ぎアクセスＳＣＰがデータベースから受信宛先情報を取得する
176
図５Ｂへ

FIG 5A

【図５】

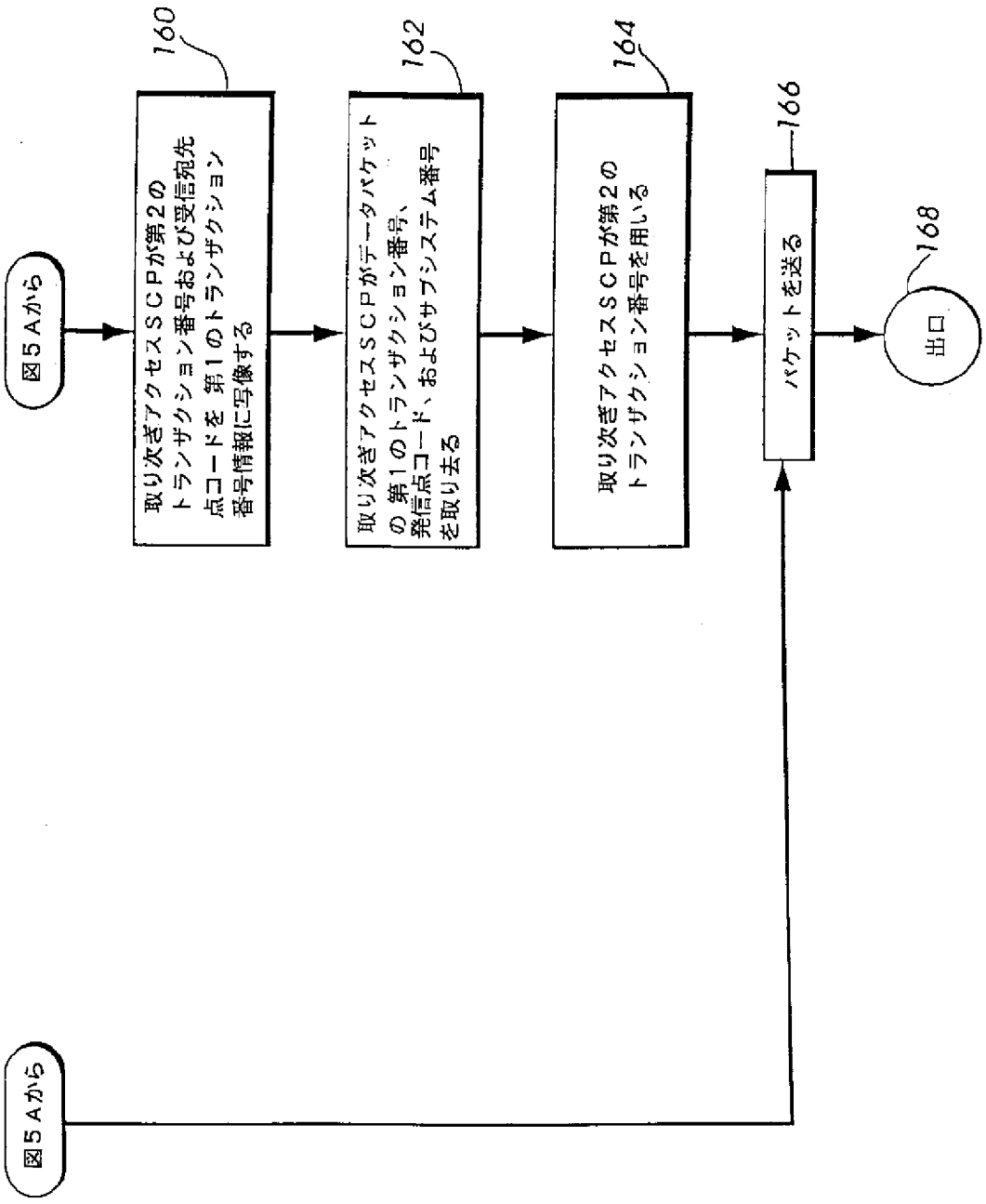
図５Ａから
160
取り次ぎアクセスＳＣＰが第２の
トランザクション番号および受信宛先
点コードを 第１のトランザクション
番号情報に写像する
162
取り次ぎアクセスＳＣＰがデータパケット
の 第１のトランザクション番号、
発信点コード、およびサブシステム番号
を取り去る
164
取り次ぎアクセスＳＣＰが第２の
トランザクション番号を用いる
166
パケットを送る
168
出口
図５Ａから

FIG 5B

【図６】

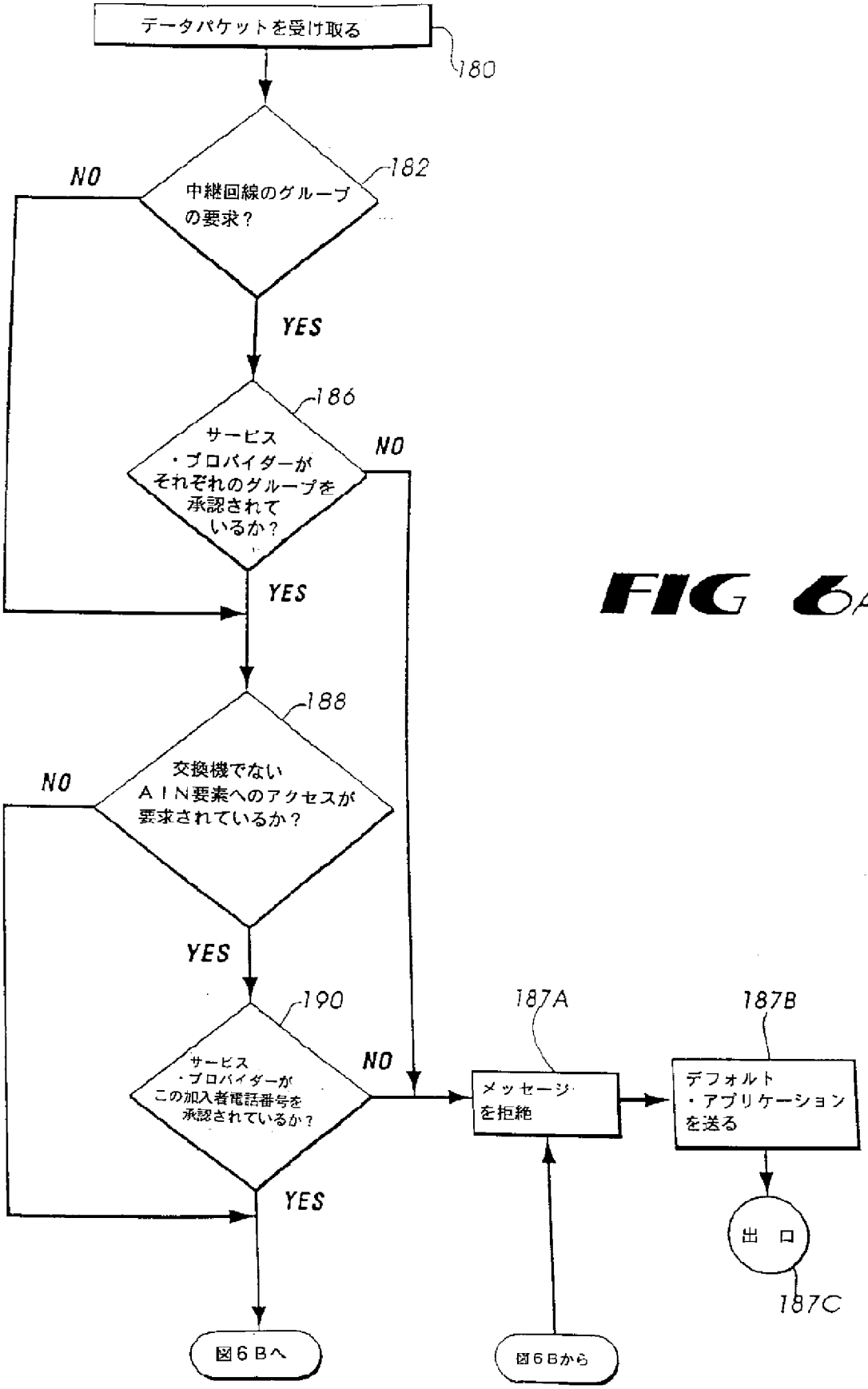
データパケットを受け取る
180
中継回線のグループの要求？
182
NO
YES
サービス・プロバイダーがそれぞれのグループを承認されているか？
186
NO
YES
交換機でないＡＩＮ要素へのアクセスが要求されているか？
188
NO
YES
サービス・プロバイダーがこの加入者電話番号を承認されているか？
190
NO
YES
メッセージを拒絶
187A
デフォルト・アプリケーションを送る
187B
出口
187C
図６Ｂへ
図６Ｂから

FIG 6A

【図６】

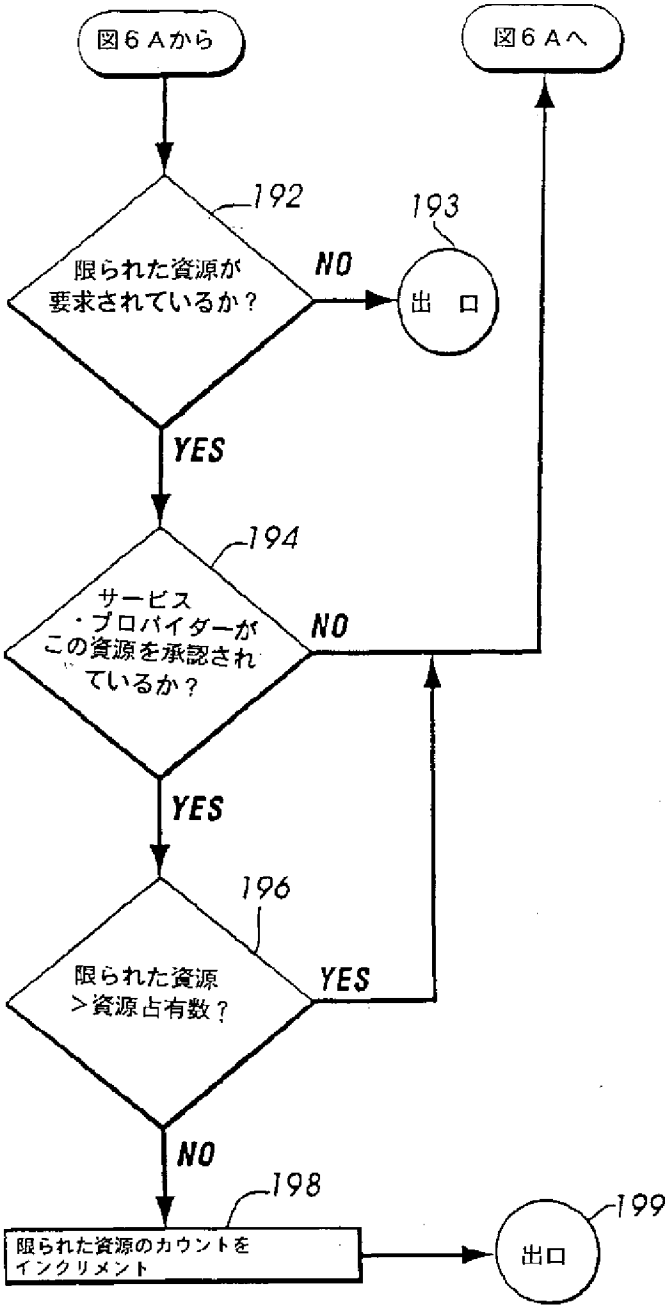
図６Ａから
図６Ａへ
192
限られた資源が
要求されているか？
NO
193
出　口
YES
194
サービス
・プロバイダーが
この資源を承認され
ているか？
NO
YES
196
限られた資源
＞資源占有数？
YES
NO
198
限られた資源のカウントを
インクリメント
199
出口

FIG 6B

【図７】

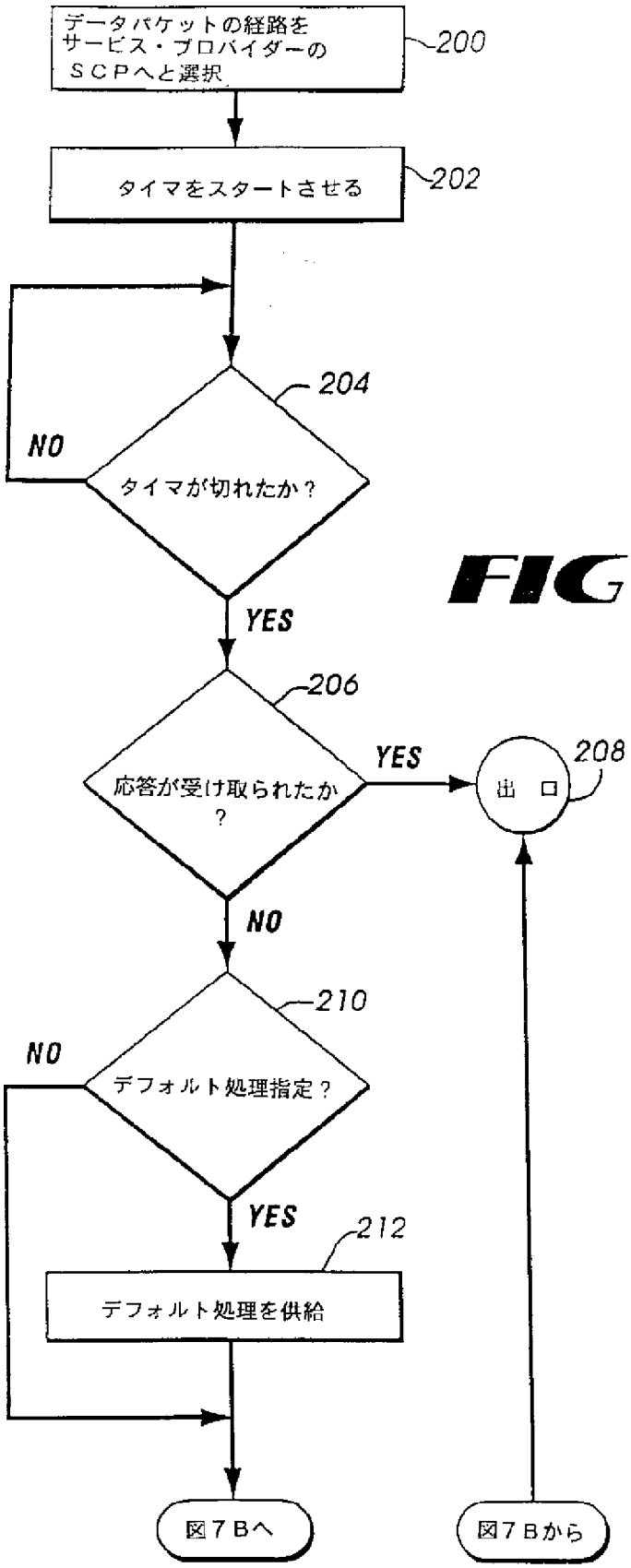
データパケットの経路を
サービス・プロバイダーの
ＳＣＰへと選択
200
タイマをスタートさせる
202
204
NO
タイマが切れたか？
YES
206
応答が受け取られたか
？
YES
208
出　口
NO
210
NO
デフォルト処理指定？
YES
212
デフォルト処理を供給
図７Ｂへ
図７Ｂから

FIG 7A

【図７】

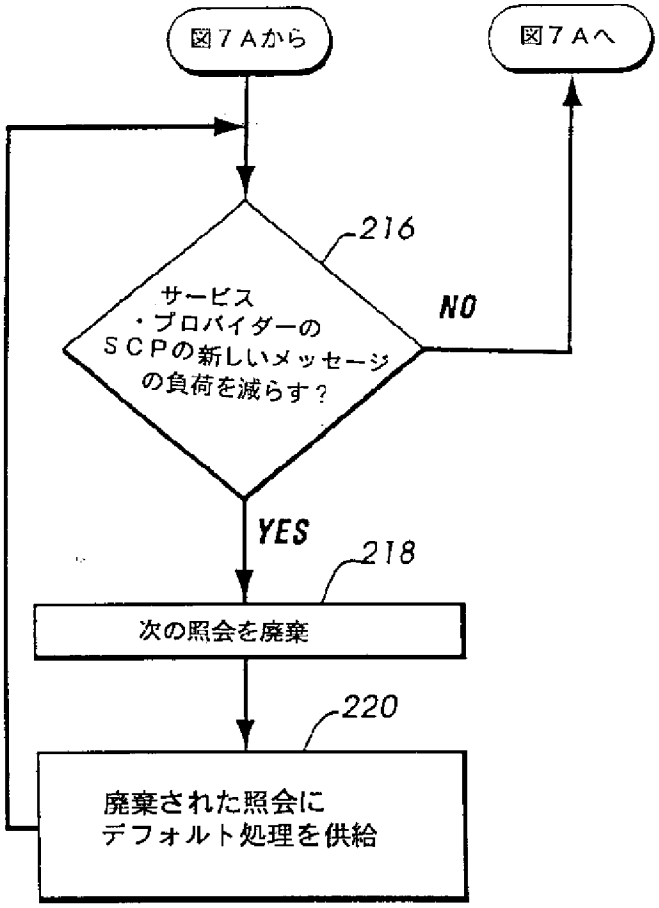
図７Ａから
図７Ａへ
216
サービス
・プロバイダーの
ＳＣＰの新しいメッセージ
の負荷を減らす？
NO
YES
218
次の照会を廃棄
220
廃棄された照会に
デフォルト処理を供給

FIG 7B

【図８】

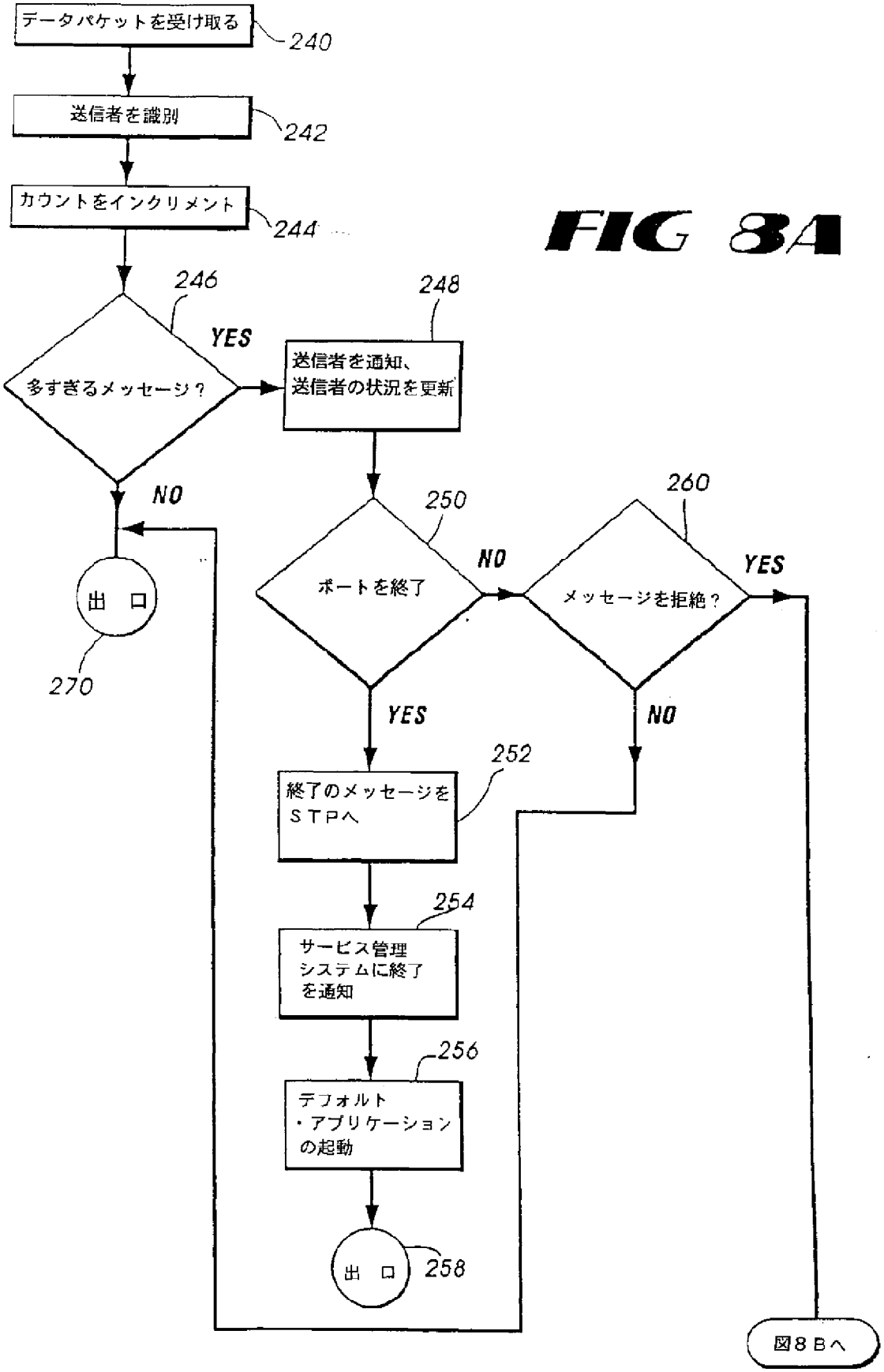
データパケットを受け取る
240
送信者を識別
242
カウントをインクリメント
244
246
YES
多すぎるメッセージ？
248
送信者を通知、
送信者の状況を更新
NO
出　口
270
250
ポートを終了
NO
260
メッセージを拒絶？
YES
YES
NO
252
終了のメッセージを
ＳＴＰへ
254
サービス管理
システムに終了
を通知
256
デフォルト
・アプリケーション
の起動
出　口
258
図８Ｂへ

FIG 8A

【図８】

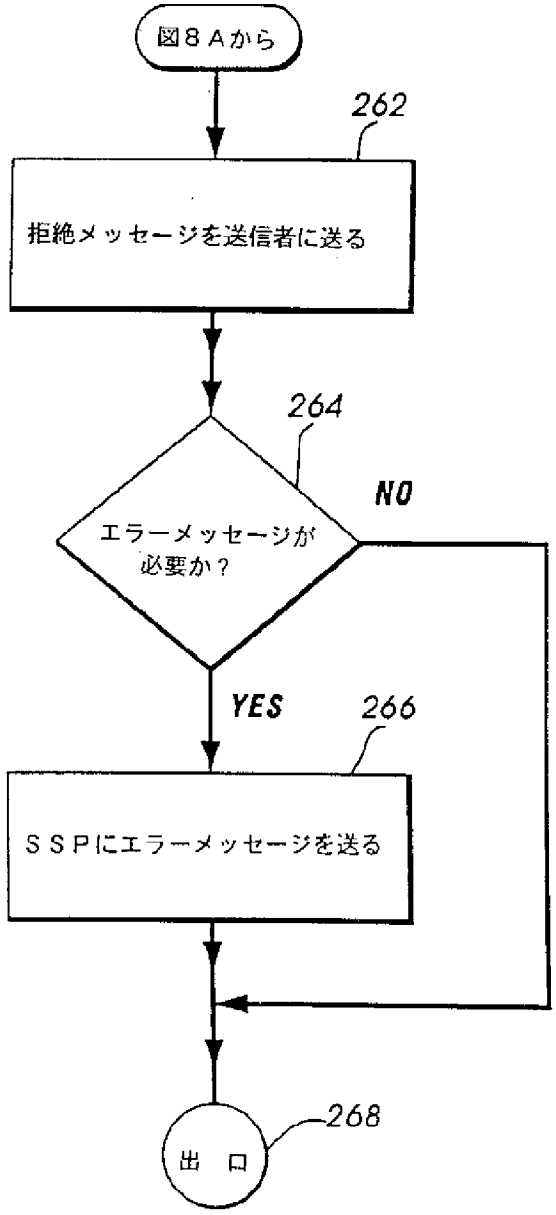
図８Ａから
262
拒絶メッセージを送信者に送る
264
エラーメッセージが
必要か？
NO
YES
266
ＳＳＰにエラーメッセージを送る
268
出　口

FIG 8B

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 95/07077

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q3/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TELEPHONY, vol.226, no.18, 2 May 1994, US pages 68 - 72 THEUS ET AL. 'Open access to the intelligent network: The road to more flexible and responsive services' see the whole document ---	1,11,14
X	IEEE NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM, vol.1, 14 February 1994, KISSIMMEE US pages 140 - 152, XP000452403 CHEN 'Open AIN operations strategies' see page 145 - page 146 --- -/--	1,11

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 October 1995	- 6. 02. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	S J LAMBLEY

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TELEPHONY, vol.226, no.22, 30 May 1994, US pages 24 - 25 JOHNSON 'Provisioning AIN services' see ---	1,8-11, 14-18
A	US,A,4 310 727 (LAWSER) 12 January 1982 see column 2, line 53 - column 3, line 56; figure 2 ---	1-4,7-9, 19-28
A	GLOBAL TELECOMMUNICATIONS CONFERENCE, vol.1, 15 November 1987, TOKYO JP pages 112 - 116 BOESE ET AL. 'The multimedia SCP' -----	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/07077

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

SEE SHEET B

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searches without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-28, 35-37

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INVITATION TO PAY ADDITIONAL FEES

International application No.
PCT/US95/07077

LACK OF UNITY OF INVENTION

1. Claims: 1-28,35-37

2. Claims: 29,30

3. Claims: 31-34

4. Claims: 38,39

5. Claims: 40-43

The common or corresponding technical feature of independent claims 1,19,25,29,30,31,32,38,40 and 42 is an intelligent switched telephone network including a mediated access service control point, or a mediation method used in such a network.

The search revealed documents 'Open access to the intelligent network: The road to more flexible and responsive services' by Theus et al., and 'Open AIN operations strategies' by Chen, each of which are considered to represent the closest prior art and disclose a network with this technical feature (see p.72, left column, lines 36 to 59; and p.145 respectively).

There are five groups of technical features claimed, which do not contain either the same or a corresponding technical feature, as they relate to different objectively determined problems and their different solutions.
These are -

A. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claims 1,19 and 25 (and their dependent claims) with respect to this prior art are - replacing certain data within an IN message with a second set of data, storing the original data, and then routing the message accordingly if data in a received message corresponds to stored data, solving the objectively determined problem of mediation of routing messages generated as a result of connection to one of a variety of service providers.

B. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claims 29 and 30 with respect to this prior art are -
checking a table of trunk route groups and a table of authorised directory numbers for correspondence to a parameter in an IN message, solving the objectively determined problem of ensuring that received parameter values correspond to values in the original data packet.

./.

C. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claims 31 and 32 (and its dependent claims) with respect to this prior art are - using a count of the occupancy of resources, and rejecting messages or introducing gapping as appropriate to prevent overload, solving the objectively determined problem of use of limited network resources offered by a service provider.

D. The special technical features, as defined in Rule 13.2 PCT, second sentence, included in claim 38 (and its dependent claim) with respect to this prior art are - sending a test message to an out-of-service SCP and re-classifying the SCP as in-service if it responds properly, solving the objectively determined problem of monitoring the status of an SCP that has been determined as out-of-service.

E. The special technical feature, as defined in Rule 13.2 PCT, second sentence, included in claims 40 and 42 (and their dependent claims) with respect to this prior art is - introducing an auditable parameter into the IN message, solving the objectively determined problem of auditing IN messages, for security or other purposes.

Consequently, the claims do not fulfill the requirement of unity (Rule 13 PCT).

INTERNATIONAL SEARCH REPORT

Information on patent family members

ernational Application No
PCT/US 95/07077

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-4310727	12-01-82	NONE	

(81)指定国　　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＫＥ，ＭＷ，ＳＤ，ＳＺ，ＵＧ)，ＡＭ，ＡＴ，ＡＵ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＥ，ＨＵ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＫ，ＬＲ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＴＪ，ＴＭ，ＴＴ，ＵＡ，ＵＧ，ＵＺ，ＶＮ

【要約の続き】
する情報に対応する情報をデータパケットから除去する。取り次ぎアクセスＳＣＰは、この除去された情報を記憶し、代用情報を生成し、除去された情報をそのデータベース内の代用情報と相関させ、データパケット内の除去された情報を代用情報と取り替える。代用情報は、データパケットの受領者にネットワークの動作に関する情報を一切供給しない。応答データパケットを受け取ると、取り次ぎアクセスＳＣＰは、応答データパケットを、代用情報を含んでいるか検査する。応答データパケットがこの代用情報を含んでいない場合には、データパケットは拒絶される。応答データパケットが代用情報を含んでおり、その他の点で妥当な場合には、取り次ぎアクセスＳＣＰは、代用情報を除去された情報と関連させ、除去された情報を用いてさらにデータパケットの経路を選択する。

【公報種別】特許法第１７条第１項及び特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成１２年３月１４日（２０００．３．１４）

【公表番号】特表平１０－５０１３９６
【公表日】平成１０年２月３日（１９９８．２．３）
【年通号数】
【出願番号】特願平８－５０２２７４
【国際特許分類第７版】
H04M　3/00
　　3/42
【ＦＩ】
H04M　3/00　　A
　　3/42　　A

手続補正書

平成１１年１０月４　日

特許庁長官殿

１．事件の表示　　平成８年特許願第５０２２７４号

２．補正をする者
　事件との関係　特許出願人
　氏名又は名称　ベルサウス　コーポレイション

３．代理人
　住　所　　〒１０５　東京都港区虎ノ門１丁目２番３号
　　虎ノ門第１ビル９階
　　電話　東京（３５０４）３０７５（代）
　氏　名　　弁理士　（８３８０）二好　靖和

４．補正の対象　　請求の範囲

５．補正の内容　　請求の範囲を別紙のとおり補正する。

特許請求の範囲

１．サービス・プロバイダーのサービス制御点（４７）およびインテリジェント交換電話ネットワーク要素の間のデータパケットメッセージの承認されない送信を防止する方法であって、

前記ネットワークは、少なくとも１つの信号中継点（２０’）を含む複数のインテリジェント交換ネットワーク要素，および少なくとも１つの取り次ぎアクセスサービス制御点（２６’）の間での複数のデジタルデータ通信チャネルを含み，顧客の記録を含む少なくとも１つのデータベース（４５）を含み、前記取り次ぎアクセスサービス制御点（２６’）が前記信号中継点（２０’）に接続されるものにおいて、

前記方法が、

前記信号中継点（２０’）内で第１のトランザクション番号を有するメッセージを受け取る手順と、

前記メッセージを前記信号中継点（２０’）から前記取り次ぎアクセスサービス制御点（２６’）へ送信する手順と、

前記取り次ぎアクセスサービス制御点（２６’）内の前記メッセージを取り次ぐ手順であって、

前記データベース（４５）内に前記メッセージの第１のトランザクション識別子を記憶することと、

前記メッセージの第２のトランザクション番号を生

成することと、

前記第２のトランザクション番号を前記データベース（４５）内の前記第１のトランザクション識別子と関連付けることと、

前記メッセージから前記第１のトランザクション番号を削除することと、

前記メッセージに前記第２のトランザクション番号を付加することと

から成る手順と

を含むことを特徴とする方法。

２．前記トランザクション識別子を記憶する前に、メッセージ情報として前記メッセージを読み取ることと、

前記メッセージ情報を前記データベース（４５）内の少なくとも１つの顧客の記録に対応するかを比較することと、

前記メッセージ情報が前記顧客の記録と対応しない場合には前記メッセージを拒否することと

をさらに含むことを特徴とする請求項１に記載の方法。

３．前記トランザクション識別子が、前記第１のトランザクション番号、前記メッセージの発信点コード、および前記メッセージのサブシステム番号を有し、

前記トランザクション識別子を記憶する手順が、前記第１のトランザクション番号、前記発信点コード、および前記サブシステム番号を記憶する手順を含むことを特徴とする請求項１に記載の方法。

４．前記メッセージが、前記第１のトランザクション番号、前記発信点コードおよび前記サブシステム番号を有し、

前記第１のトランザクション番号を削除する手順が前記第１のトランザクション番号、前記発信点コード、および前記サブシステム番号を前記メッセージから削除する手順を含むことを特徴とする請求項３に記載の方法。

５．前記データベース（４５）内で活動状態にある第２のトランザクション番号のリストに前記第２のトランザクション番号を記憶する手順をさらに含むことを特徴とする請求項２に記載の方法。

６．前記第２のトランザクション番号は割り当てられていない疑似乱数であり、前記第２のトランザクション番号を生成する前記手順が前記割り当てられていない疑似乱数を前記第２のトランザクション番号として生成する手順を含むことを特徴とする請求項２に記載の方法。

７．前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次く手順が、

前記メッセージが応答メッセージかどうかを決定する手順と、

前記メッセージが応答メッセージである場合には、前記応答メッセージのトランザクション番号を前記データベース（４５）に記憶されている活動状態のトランザクション番号のリストに対応するか比較する手順と、

前記トランザクション番号が前記活動状態のトランザクション番号のリスト内の登録内容と対応しない場合には、前記メッセージを拒否する手順と

を含むことを特徴とする請求項１に記載の方法。

８．前記トランザクション番号が活動状態のトランザクション番号の前記リストの登録内容に対応する場合には、前記登録内容から受信宛先情報を取得する手順と、

前記受信宛先情報に基づいて前記メッセージの経路を決定する手順と、

をさらに含むことを特徴とする請求項７に記載の方法。

９．前記取り次ぎアクセスサービス制御点内の前記メッセージを取り次く手順が、

前記メッセージが照会メッセージに応答して前記サービス・プロバイダーのサービス制御点（４７）から受け取る応答メッセージであるどうかを決定する手順と、

前記メッセージが応答メッセージの場合には前記応答メッセージが発信点コードを含むかどうかを決定する手順と、

前記応答メッセージが前記発信ポイントコードを含む場合には、前記発信点コードが前記照会メッセージに関連した受信宛先点コードに対応するかを比較する手順と、

前記発信点コードが前記受信宛先点コードに対応しない場合には、前記メッセージを拒否する手順と、

をさらに含むことを特徴とする請求項１に記載の方法。

１０．前記取り次ぎアクセスサービス制御点（２６'）の前記メッセージを取り次く前記手順のあとに、前記メッセージが前記取り次ぎアクセスサービス制御点（２６'）内の取り次ぎを通過したかどうかを決定する手順と、

前記メッセージが前記取り次ぎアクセスサービス制御点（２６'）内の取り次ぎを通過した場合には、前記サービス・プロバイダーのサービス制御点（４７）がサービス外であるかどうかを決定する手順と、

前記サービス・プロバイダーのサービス制御点（４７）がサービス外の場合には、前記メッセージを拒否し、前記メッセージをデフォルト応答で提供する手順と、

をさらに含むことを特徴とする請求項１に記載の方法。

１１．前記メッセージが特定のサービス・プロバイダーのサービスの要求を含み、

前記サービス・プロバイダーのサービス制御点（４７）がサービス外であるかどうかを決定する前記手順が、

前記特定のサービス・プロバイダーのサービスがサービス外であるかどうかを決定する手順と、

前記特定のサービス・プロバイダーのサービスがサービス外である場合には、前記メッセージを拒否し、前記メッセージを前記デフォルト応答で提供する手順と

を含むことを特徴とする請求項１０に記載の方法。

１２．前記信号中継点（２０'）内で前記メッセージを受け取る前記手順のあとに、前記メッセージを前記プロバイダーのサービス制御点（４７）から発信するかどうかを決定する手順と、

前記メッセージを前記プロバイダーのサービス制御点（４７）から発信する場合には、前記信号中継点（２０'）内の前記メッセージを最初に取り次ぐ手順と

をさらに含むことを特徴とする請求項１に記載の方法。

１３．前記メッセージが発信点コードを備え、

前記信号中継点（２０'）が前記信号中継点（２０'）へのメッセージの各承認されたプロバイダーのポート識別子を有し、

前記信号中継点（２０'）で前記メッセージを最初に取り次ぐ手順が、

前記発信点コードを少なくとも１つのポート識別子に対応するか比較することと、

前記発信点コードが前記ポート識別子のいずれにも対応しない場合には、前記メッセージを拒否することとを含むことを特徴とする請求項１２に記載の方法。

１４．前記メッセージが受信宛先コードを含み、

前記信号中継点（２０'）が、前記信号中継点（２０'）へのメッセージの各承認されたプロバイダーのメッセージ承認された受信宛先を指定する少なくとも１つの承認されたアドレスを有し、

前記信号中継地点（２０'）内で前記メッセージを最初に取り次ぐ前記手順が、

前記受信宛先コードが少なくとも１つの承認されたアドレスに対応するかを比較するする手順と、

前記受信宛先コードが前記承認されたアドレスのいずれにも対応しない場合には前記メッセージを拒否する手順とを含む

ことを特徴とする請求項１２に記載の方法。

１５．前記承認されたアドレスの１つが前記取り次ぎアクセスサービス制御点のアドレスを含み、

前記比較する手順が、前記受信宛先コードが前記取り次ぎアクセスサービス制御点（２６'）の前記アドレスに対応するか比較することを含み、

前記拒否する手順が、前記受信宛先コードが前記取り次ぎアクセスサービス制御点（２６'）の前記アドレスに対応しない場合には前記メッセージを拒否することを含むことを特徴とする請求項１４に記載の方法。

１６．前記メッセージがサービスインジケータを有し、前記信号中継点（２０'）は、前記信号中継点（２０'）へのメッセージのそれぞれの承認されたプロバイダーの承認されたサービスを指定する少なくとも１つのサービスインジケータを有し、

前記信号中継点（２０'）内の前記メッセージを最初に取り次ぐ手順が、

前記サービスインジケータが少なくとも１つの承認されたサービスインジケータに対応するか比較すること、および

前記サービスインジケータが前記承認されたサービスインジケータのいずれにも対応しない場合には、前記メッセージを拒否すること

を含むことを特徴とする請求項１２に記載の方法。

１７．複数のネットワーク要素間の複数のデジタル通信チャネルを備えるインテリジェント交換電話ネットワークにおいてパケットメッセージのトラヒックを取り次く方法において、前記方法が、

新しいトランザクション性能アプリケーション部メッセージを生成する前記複数のネットワーク要素の第１のものに、各前記新しいトランザクション性能アプリケーション部メッセージの第１のトランザクション番号を発生させる手順と、

前記第１のネットワーク要素が前記複数のネットワーク要素のうち第２のものに前記トランザクション性能アプリケーション部メッセージを送信する前に、前記第１のネットワーク要素に、前記第１トランザクション番号を前記トランザクション性能アプリケーション部メッセージに含ませる手順と、

前記第２のネットワーク要素に、前記トランザクション性能アプリケーション部メッセージに関連した単一のトランザクション識別子を生成させる手順と、

前記第２のネットワーク要素に、前記トランザクション性能アプリケーション部メッセージの第２のトランザクション番号を発生させる手順と、

前記第２のネットワーク要素に、前記トランザクション性能アプリケーション部メッセージから前記第１のトランザクション番号を削除させる手順と、

前記ネットワーク要素が前記トランザクション性能アプリケーション部メッセージを別の受信宛先に送信する前に、前記第２のネットワーク要素に、前記トランザクション性能アプリケーション部メッセージ内に前記第２のトランザクション番号を含ませる手順と、

前記トランザクション性能アプリケーション部メッセージと関連する特定のトランザクションには影響を与えるが内部には前記第２のトランザクション番号を含まない他のトランザクション性能アプリケーション部メッセ

－ジを前記ネットワーク要素にその後拒否させる手順と、
を含むことを特徴とする方法。

１８．前記第１のネットワーク要素に、トランザクション識別子のテーブル内に前記第１のトランザクション番号を記憶させる手順をさらに含むことを特徴とする請求項１７に記載の方法。

１９．前記第２のネットワーク要素に、前記単一のトランザクション識別子をトランザクション識別子テーブル内に記憶させることと、
第２のネットワーク要素に、前記単一のトランザクション識別子に関連した前記トランザクション識別子テーブル内に前記第２のトランザクション番号を記憶させることと、
を含むことを特徴とする請求項１７に記載の方法。

２０．前記第１のネットワーク要素に前記第１のトランザクション番号を含ませる前記手順が、
前記第１のネットワーク要素に、前記第１のトランザクション番号およびメッセージ識別子を前記トランザクション性能アプリケーション部メッセージ内に含ませること
を含んで構成されることを特徴とする請求項１７に記載の方法。

２１．前記トランザクション性能アプリケーション部メッセージが、発信点コード、およびサブシステム番号を有し、
前記第２のネットワーク要素に前記単一のトランザクション識別子を生成させる手順が、
前記第２のネットワーク要素に、前記第１のトランザクション番号を前記発信点コードおよび前記サブシステム番号と連結することにより前記単一のトランザクション識別子を生成させること
を特徴とする請求項１７に記載の方法。

２２．前記第２のネットワーク要素に前記第１のトランザクション番号を削除させる手順が、前記第２のネットワーク要素に、前記トランザクション性能アプリケーション部メッセージから前記第１のトランザクション番号、前記発信点コード、および前記サブシステム番号を削除させることを特徴とする請求項２１に記載の方法。

２３．サービス・プロバイダーのサービス制御点（４７）および複数のネットワーク要素間の複数のデジタルデータ通信を含むインテリジェント交換電話ネットワークの間のパケットメッセージのトラヒックを取り次ぐ方法において、前記方法が、

第１のトランザクション番号を有するメッセージを受信するネットワーク要素に、前記メッセージに関連した単一のトランザクション識別子を生成させることと、
前記ネットワーク要素に、前記メッセージの第２のトランザクション番号を発生させることと、
前記ネットワーク要素に、前記単一のトランザクション識別子に関連した第２のトランザクション番号を記憶させることと、
前記ネットワーク要素に、前記メッセージから前記第１のトランザクション番号を削除させることと、
前記ネットワーク要素に前記メッセージに前記第２のトランザクション番号を付加させることと、
前記サービス・プロバイダーのサービス制御点（４７）および前記ネットワーク要素に、その後、前記メッセージに関連した特定のトランザクションに影響を与える他のメッセージ内に前記第２のトランザクション番号を含ませ、前記第２のトランザクション番号を含まない前記他のメッセージを拒否させること
を含むことを特徴とする方法。

２４．前記メッセージが発信点コードを含み、前記ネットワーク要素が前記ネットワークへのメッセージの各承認されたプロバイダーのポート識別子を備え、
前記方法が、
前記ネットワーク要素に、前記発信点コードをポート識別子に対応して比較させること、および
前記ネットワーク要素に、前記発信点コードが前記ポート識別子のいずれにも対応しない場合には前記メッセージを拒否させること
をさらに含むことを特徴とする請求項２３に記載の方法。

２５．前記メッセージが受信宛先コードを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーのメッセージの承認された受信宛先を指定する少なくとも１つの承認されたアドレスを有し、
前記ネットワーク要素に、前記受信宛先コードが少なくとも１つの承認されたアドレスに対応するか比較させる手順と、
前記受信宛先コードが前記承認されたアドレスのいずれにも対応しない場合には、前記ネットワーク要素に前記メッセージを拒否させる手順と、
を含むことを特徴とする請求項２３に記載の方法。

２６．前記メッセージがサービスインジケータを含み、前記ネットワーク要素が前記ネットワーク要素へのメッセージの各承認されたプロバイダーの承認されたサービスを指定する少なくとも１つのサービスインジケータを有し、

前記ネットワーク要素に，前記サービスインジケータが少なくとも１つの承認されたサービスインジケータに対応するか比較させる手順と，

前記サービスインジケータが前記承認されたサービスインジケータに対応しない場合には，前記ネットワーク要素に前記メッセージを拒否させる手順と

を含むことを特徴とする請求項２３に記載の方法。

２７．サービス・プロバイダーのサービス制御点（４７）および取り次ぎアクセスサービス制御点（２６'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において，前記方法が，

前記取り次ぎアクセスサービス制御点（２６'）に，前記サービス・プロバイダーのサービス制御点（４７）の特定の中継回線のグループインデックスのテーブルを維持させる手順と，

前記取り次ぎアクセスサービス制御点（２６'）が前記特定の中継回線の経路要求を含むメッセージを受け取ることに応答して，前記取り次ぎアクセスサービス制御点（２６'）に，前記特定の中継回線のグループの経路に対応する登録内容の前記テーブルをチェックさせる手順と，

前記特定の中継回線のグループの経路が前記テーブル内の登録内容に対応しない場合には，前記取り次ぎアクセスサービス制御点（２６'）に前記メッセージを拒否させる手順と

を含むことを特徴とする方法。

２８．サービス・プロバイダーのサービス制御点（４７），および取り次ぎアクセスサービス制御点（２６'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において，

前記取り次ぎアクセスサービス制御点（２６'）に，前記サービス・プロバイダーのサービス制御点（４７）のネットワーク要素の承認された加入者電話番号のテーブルを維持させる手順と，

前記取り次ぎアクセスサービス制御点（２６'）がネットワーク要素へのアクセスの要求を含むメッセージを受け取ることに応答して，前記取り次ぎアクセスサービス制御点（２６'）に，前記ネットワーク要素の加入者電話番号に対応する登録内容の前記テーブルをチェックさせる手順と，

前記加入者電話番号が前記テーブル内の登録内容に対応しない場合には，前記取り次ぎアクセスサービス制御点（２６'）に前記メッセージを拒否させる手順と，

を含むことを特徴とする方法。

２９．サービス・プロバイダーのサービス制御点（４７）および取り次ぎアクセスサービス制御点（２６'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において，前記方法は，

前記取り次ぎアクセスサービス制御点（２６'）に，前記サービス・プロバイダーのサービス制御点（４７）の許された資源占有数を維持させる手順と，

前記取り次ぎアクセスサービス制御点（２６'）に，前記サービス・プロバイダーのサービス制御点（４７）が占有している資源の現在のカウントを維持させる手順と，

前記取り次ぎアクセスサービス制御点（２６'）がネットワーク資源の使用の要求を含むメッセージを受け取ることに応答して，前記現在のカウントが前記許された資源占有数と等しいかそれより大きい場合には，前記取り次ぎアクセスサービス制御点（２６'）に前記メッセージを拒否させる手順と

を含むことを特徴とする方法。

３０．サービス・プロバイダーのサービス制御点（４７）および取り次ぎアクセスサービス点（２６'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において，前記方法は，

前記取り次ぎアクセスサービス点（２６'）に，前記サービス・プロバイダーのサービス制御点（４７）が所定の時間内に戻さないメッセージの現在のカウントを維持させる手順と，

前記現在のカウントが所定のカウントと等しいかそれを上回った場合には，前記取り次ぎアクセスサービス点（２６'）に前記サービス・プロバイダーのサービス制御点（４７）に提供されるメッセージの数を減少させる手順と

を含むことを特徴とする方法。

３１．前記取り次ぎアクセスサービス点（２６'）にメッセージの数を減少させる前記手順が，前記取り次ぎアクセスサービス点（２６'）に，前記サービス・プロバイダーのサービス制御点（４７）宛ての次のメッセージを拒否させる手順を含むことを特徴とする請求項３０に記載の方法。

３２．前記ネットワークが前記サービス・プロバイダーのサービス制御点（４７）をサービスする少なくとも１つのサービス交換点（１５）を含み，

前記取り次ぎアクセスサービス点（２６'）にメッセージ数を減少させる前記手順が，前記取り次がれたアクセスサービス制御点（２６'）に自動発呼ギャッピングのメッセージを前記サービス交換点（１５）に送らせる手順を含むことを特徴とする請求項３０に記載の方法。

３３．サービス外のサービス・プロバイダーのサービス制御点を試験する手順と、

前記サービス外のサービス・プロバイダーのサービス制御点が前記試験に適切に応答した場合には、前記サービス外のサービス・プロバイダーのサービス制御点をサービス中のサービス・プロバイダーのサービス制御点として再分類する手順と

をさらに含むことを特徴とする請求項１０に記載の方法。

３４．前記サービス外のサービス制御点を試験する前記手順が、前記サービス外のサービス・プロバイダーのサービス制御点に試験メッセージを送る手順を含むことを特徴とする請求項３３に記載の方法。

３５．前記サービス外のサービス制御点を試験する前記手順が、前記サービス外のサービス・プロバイダーのサービス制御点に試験メッセージを定期的なベースで送る手順を含むことを特徴とする請求項３４に記載の方法。

３６．サービス外のサービス・プロバイダーのサービス制御点および取り次ぎアクセスサービス点（２６'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法が、

前記サービス外のサービス・プロバイダーのサービス制御点（２６'）に試験メッセージを送ることと、

前記サービス外のサービス・プロバイダーのサービス制御点が適切に前記試験メッセージで応答した場合には、前記サービス外のサービス・プロバイダーのサービス制御点をサービス中のサービス・プロバイダーのサービス制御点として再分類することと

を含むことを特徴とする方法。

３７．前記サービス外のサービス制御点に試験メッセージを送る手順が、前記サービス外のサービス・プロバイダーのサービス制御点に定期的に試験メッセージを送ることを特徴とする請求項３６に記載の方法。

３８．サービス・プロバイダーのサービス制御点（４７）および取り次ぎアクセスサービス点（２６'）を含むインテリジェント交換電話ネットワークの間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法が、

前記取り次ぎアクセスサービス点（２６'）に、データパケットメッセージ内の前記取り次がれたトラヒックについての監査可能な事象を認識させる手順と、

前記監査可能な事象の監査証跡を生成する手順と

を含むことを特徴とする方法。

３９．前記監査可能な事象がメッセージを含み、前記監査証跡が前記メッセージの日付、時刻、トリガのタイプ、トリガする宛先番号、および前記メッセージのコピーから構成され、

前記監査可能な事象の監査証跡を生成する手順が、前記メッセージの前記日付、前記時刻、前記トリガのタイプ、トリガする前記宛先番号、および前記メッセージの前記コピーを含む前記監査証跡を生成することから成ることを特徴とする請求項３８に記載の方法。

４０．サービス・プロバイダーのサービス制御点（４７）およびインテリジェント交換電話ネットワークの複数のネットワーク要素の間のデータパケットメッセージの取り次がれたトラヒックを管理する方法において、前記方法が、

前記ネットワーク要素の１つでセキュリティ監査要求パラメータを含むメッセージを受信することと、

前記セキュリティ監査要求パラメータを受信することに応答して、前記ネットワーク要素の前記１つに前記メッセージのセキュリティパラメータを生成させることと

を含むことを特徴とする方法。

４１．前記ネットワーク要素に、その後、前記メッセージに関連する特定のトランザクションに影響を与える他のメッセージとともに前記セキュリティパラメータを保持させる手順をさらに含むことを特徴とする請求項４０に記載の方法。